ZoneAlarm by Check Point SOFTWARE TECHNOLOGIES LTD.

ZoneAlarm 2012

versions 10.*x*

User Guide

PDF version of Online Help Center

©2011 Check Point Software Technologies Ltd. All rights reserved.

Contents

Welcome 6

ZoneAlarm User Forum 6

ZoneAlarm security software basics 6

Getting started with ZoneAlarm 6
Firewall zone basics 9
Responding to alerts 11
Configuration 12
Setting product preferences 13
Setting product update options 15
Licensing, registration, and support 15
About updating from a prior version 16
Moving to a different computer 17
Uninstalling ZoneAlarm 17

Configuring for networks and resources 17

Configuring a new network connection 17
Integrating with network services 19
Configuring your VPN connection 20

Firewall protection 24

Understanding Firewall protection 24
Choosing security levels 25
Setting advanced security options 26
Managing traffic sources 29
Blocking and unblocking ports 32
Understanding expert firewall rules 35
Creating expert firewall rules 36
Creating groups 39
Managing Expert Firewall Rules 43

Understanding and reducing alerts 46

About alerts and managing them 46
Informational alerts 47

Program alerts **62**
OSFirewall alerts **88**
ID Lock alert **97**

Application Control **100**

Understanding Application Control **100**
Setting general program control options **103**
Setting permissions for specific programs **111**
Setting program options for a specific program **116**
Managing program components **118**
Creating expert rules for programs **119**

Browser security **120**

Using browser security **120**
Spyware and virus Protection **121**
Customizing virus protection options **123**
Performing a scan **129**
Viewing virus and spyware protection status **134**
Monitoring virus protection **135**

E-mail protection **138**

Understanding e-mail protection **138**
Customizing Outbound MailSafe protection **139**
Filtering junk e-mail (spam) **140**
Understanding the ID Lock feature **149**
About myVAULT **152**
Using the Trusted Sites list **154**
Identity Protection Center (US only) **156**
What Hard Drive Encryption does for you **157**
Installing ZoneAlarm DataLock **157**
Using ZoneAlarm DataLock **157**
Troubleshooting ZoneAlarm DataLock **158**

Managing Alerts and Logs **159**

Understanding alerts and logs **160**
Showing or hiding firewall and program alerts **160**
Setting basic alert and log options **161**
Controlling the number of alerts **162**
Setting event and program log options **162**
Using SmartDefense Advisor and Hacker ID **167**

Game Mode 168

Understanding Game Mode 168
Turning Game Mode On and Off 169

Troubleshooting 170

Troubleshooting VPN 170
Troubleshooting networking 171
Troubleshooting an Internet disconnection 173
Troubleshooting Anti-virus 175
Troubleshooting Hard Drive Encryption 177
Troubleshooting third-party software Internet access 177

Keyboard shortcuts 184

Global function shortcuts 184
Dialog box commands 184
Button shortcuts 185

Index 189

Welcome

Welcome to ZoneAlarm security software, the easy-to-use Internet security program that protects you from known and unknown threats.

Quick Links:

- Getting started ("Getting started with ZoneAlarm" on page 6)
- Top 10 user questions
- Troubleshooting (on page 170)
- Some features are only in premium products

ZoneAlarm User Forum

Connect with other users of ZoneAlarm security software. Ask questions, get answers, and see how fellow users get the most out of their ZoneAlarm security software. Visit the user forum , http://forums.zonealarm.com/.

ZoneAlarm security software basics

ZoneAlarm security software is preconfigured to provide protection as soon as you install it, and will alert you if it needs anything from you. The topics in this section provides an introduction to the main tools and concepts of ZoneAlarm security software.

Getting started with ZoneAlarm

If ZoneAlarm security software is installed and running, there is nothing you need to configure in order to start being protected— it alerts you if it needs your attention.

If you want to explore the features and options, the topics in this section are a good place to start.

Overview of main features

This table introduces the main features in ZoneAlarm.

Note - Some features listed below are only in premium versions of the product.

Feature	Feature Description
Inbound Firewall	Protects your computer from dangerous intrusions by guarding the "doors" (network ports) to your computer. The default settings defend you against unauthorized intrusions. Advanced users can customize firewall configurations. For more information, see Firewall protection (on page 24).
Application Control	Protects you against criminal programs that would send your personal data over the Internet. Ensures that only programs you trust access the Internet. Also, OS Firewall alerts you if programs try to perform suspicious actions. If ZoneAlarm does not recognize a program, it asks you what access you want to give to it. For more information, see Application Control. ("Application Control" on page 100)
Anti-virus and Antispyware	Detects and treats malicious programs called viruses and spyware. Checks your system against constantly updated databases of known viruses and spyware. Detects virus or spy-like behaviors such as self-modifying, self-replicating, data capturing, and port altering. For more information, see Virus and spyware protection (on page 121).
Parental Controls	The Parental Controls help you block content that is not appropriate for your kids. For more information, see Parental Controls (on page 137).
Browser Security	ZoneAlarm browser security protects your personal data, privacy, and PC from threats that come through your Web browser. Defends against malicous downloads, browser exploits, phishing, and spyware. Some versions include a Private Browser option that "leaves no trace" behind on your computer. See Using ZoneAlarm browser security ("Using browser security" on page 120).
E-mail Protection	Protects the people in your e-mail address book by halting outbound email that displays virus-like activity. The Junk E-mail Filter removes unwanted spam mail from your inbox, and can

Feature	Feature Description
	prevent identity theft by deleting phishing email. For more information, see E-mail protection (on page 138).
Identity Protection	You can put your personal data into a virtual "vault" (called myVAULT) to keep it safe from hackers and ID thieves. Then set Identity Lock to Medium or High to protect your vault data. Some versions of the product also include a button for signing up for offline identity protection. Additional Identity Protection Services are available. For more information, see Identity protection (on page 149).

Notification icons and shortcut menus

The ZoneAlarm icons displayed in the Windows Taskbar notification tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks.

Notification icons

Icon	Description
	ZoneAlarm security software is installed and running.
	ZoneAlarm security software is running a spyware and/or virus scan. For details about scans, see Performing a scan.
	ZoneAlarm security software is receiving an anti-virus signature update.

Notification shortcut menu

Right-click any of the notification icons to access a shortcut menu.

Menu item	Description
Show Monitor	Opens the ZoneAlarm interface.
Scan Now/View Scan	Starts a system virus scan or displays the Scanning Status dialog box, which tracks the progress of spyware and virus scans and allows you to pause or cancel a scan.
Update Now	Updates your antivirus detection to that it can detect the latest threats. This is done quietly and does not interrupt your work or require a reboot.
Help	Displays the Help Center, which includes Troubleshooting and a Tutorial link.
Game Mode / Stop Game Mode	Opens the dialog that controls Game Mode. When activated, Game Mode suppresses ZoneAlarm updates, scans, and most alerts. You choose whether to deny or allow all program and network permission requests while Game Mode is active. For details about this feature, see Game Mode (on page 168).
About	Displays version information for the ZoneAlarm security software you have installed, including driver and engine information. If you are experiencing problems with your software you can copy this information to the clipboard and paste it into an e-mail to support.

Notification Tray Shortcut Menu

Firewall zone basics

ZoneAlarm security software keeps track of the good, the bad, and the unknown out on the Internet by using virtual containers, called Zones, to classify the computers and networks that connect to your computer.

The **Public (Internet) Zone** is the "unknown." All the computers and networks in the world belong to this Zone—until you move them to one of the other Zones.

The **Trusted Zone** is the "good." It contains all the computers and networks you trust and want to share resources with—for example, the other machines on your local or home network.

The **Blocked Zone** is the "bad." It contains computers and networks you distrust.

When another computer wants to communicate with your computer, ZoneAlarm security software looks at the Zone it is in to help decide what to do.

To learn how to put a computer, network, or program in the Trusted Zone, see Managing traffic sources (on page 29).

- Zones manage firewall security (on page 10)
- Zones provide Application Control as outbound protection

Zones manage firewall security

ZoneAlarm security software uses security levels to determine whether to allow or block inbound traffic from each Zone. Use the **Firewall** panel to view and adjust security levels.

High security setting

High security places your computer in stealth mode, making it invisible to hackers. High security is the default configuration Public Zone.

In High security, file and printer sharing is disabled; but outgoing DNS, outgoing DHCP, and broadcast/multicast are allowed, so that you are able to browse the Internet. All other ports on your computer are closed except when used by a program that has access permission and/or server permission.

Medium security setting

Medium security places your computer in component learning mode, where ZoneAlarm security software quickly learn the MD5 signatures of many frequently used program components without interrupting your work with multiple alerts. Medium security is the default setting for the Trusted Zone.

In Medium security, file and printer sharing is enabled, and all ports and protocols are allowed. (If Medium security is applied to the Public Zone, however, incoming NetBIOS traffic is blocked. This protects your computer from possible attacks aimed at your Windows networking services.) At Medium security, you are no longer in stealth mode.

No security level is necessary for the Blocked Zone, because no traffic to or from that Zone is allowed.

Note - Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. For more information, see Blocking and unblocking ports (on page 32).

Zones provide Application Control as outbound protection

Whenever a program requests access permission or server permission, it is trying to communicate with a computer or network in a specific Zone. For each program you can grant or deny the following permissions:

- Access permission for the Trusted Zone.
- Access permission for the Public Zone.
- Server permission for the Trusted Zone.
- Server permission for the Public Zone.

By granting access or server permission for the Trusted Zone, you enable a program to communicate only with the computers and networks you have put in that Zone. This is a highly secure strategy. Even if a program is tampered with, or given permission accidentally, it can only communicate with a limited number of networks or computers.

By granting access or server permission for the Public Zone, however, you enable a program to communicate with any computer or network, anywhere.

Note - Advanced users can specify the ports and protocols a particular program can use, the hosts it can access, and other details. For more information, see Creating an expert rule for a Program.

Responding to alerts

When you first start using ZoneAlarm security software, it is not unusual to see a number of Program or New Network alerts. Don't worry! This doesn't mean you're under attack. It just means that ZoneAlarm security software is learning your program and network configurations, and giving you the opportunity to set up your security the way you want it.

If ZoneAlarm is alerting you about an application's behavior, it's because it's one of the rare programs that our community-powered DefenseNet doesn't have enough data about yet.

In general, we recommend this cautious strategy:

Do you trust the application and what it's trying to do?

- **If yes**, click Allow.
- **If you aren't sure**, do an Internet Search on the application name to see if you can verify its trustworthiness. Sometimes the name sounds obscure, but turns out to be part of an application you use and trust.
- **If you still aren't sure**, jot down the application name (you may need it momentarily) and then click Deny, just to be safe.

- **If you click Deny**, but soon afterward your application seems to be blocked from working correctly, use the Application Control settings to restore its Internet access privileges:
  a) In ZoneAlarm, select **Computer | Details** or click the **Computer** tab.
  b) Select **Application Control | Settings**.
  c) Click **Advanced Settings**, then click **View Programs**.
  d) Select the application in the list give it Access permissions by selecting **Allow** from the popup menu.

For more about the different types of alerts you may see, and to find out what you can do to see fewer of them, use Understanding and reducing alerts **(on page 46).**

Configuration

After installation, your ZoneAlarm security software is already configured and there is nothing more you must do. If you like, there are some customizations you can make.

Customizing program Internet access permissions

While ZoneAlarm security software automatically sets permissions that specify which programs can transmit information across your firewall, you have the option of customizing these permissions for your applications.

To learn how, see Setting permissions for specific programs (on page 111).

The DefenseNet community

ZoneAlarm security software users help keep themselves and other users safer by being in the DefenseNet community protection network. You are in this network by default, and it periodically collects anonymous threat data for analysis.

The data collected is completely anonymous and is for ZoneAlarm internal use only and will not be shared with others. Of the millions of ZoneAlarm security software users, only a small percentage of users will have their information collected. The frequency of data transmission depends upon the configuration of your computer. For most users, data will be sent once per day.

To control your DefenseNet participation:

- From the **Tools** menu, choose **Preferences**.
- In the **Contact with ZoneAlarm** area, select or deselect **Share my security settings anonymously with ZoneAlarm**.

Product preferences

See Setting product preferences (on page 13) to find out how to set or change your ZoneAlarm security software password, and set general options for the display of ZoneAlarm security software.

Setting product preferences

Use the Preferences panel to set or change a ZoneAlarm security software password, configure a proxy server, back up or restore ZoneAlarm security software settings, or register your product.

Setting your password

By setting a password, you prevent anyone but you from shutting down or uninstalling ZoneAlarm security software, or changing your security settings. Setting a password will not prevent other people from accessing the Internet from your computer.

If your version of ZoneAlarm security software was installed by an administrator with an installation password, that administrator can access all functions.

When you set a password for the first time, be sure to log out before leaving your computer. Otherwise, others can still change your settings.

To set or change a ZoneAlarm security software password:

1. Select **Tools** | **Preferences**.
2. Click **Set Password**.
3. Type your password and password verification in the fields provided.
4. Select **Allow others to use programs without a password** (unless the program permission is set to "Block") to allow others to use programs you haven't explicitly blocked, even if they don't have a password.
5. Click **OK**.

Note - Valid passwords are between 6 and 31 characters long. Valid characters include A-Z, a-z, 0-9, and characters !,@,#,$,%,^,&,*.

Once you have set a password, you must log in before you can change settings, shut down the TrueVector security engine, or uninstall ZoneAlarm security software.

Backing up and restoring your ZoneAlarm settings

You can back up your existing settings to an XML file so that you can restore them later or use the same settings on another computer, should you need to.

Note - The backup and restore feature should not be used to share settings among different computers or to distribute security policies. To do so could cause an extremely high number of unecessary alerts to appear due to differences among computers, applications, and Windows processes.

To back up your ZoneAlarm security settings

1. From the **Tools** menu, choose **Preferences**.
2. In the Backup and Restore area, click **Backup**.
3. Type a file name or select an existing file to overwrite.
4. Click **Save**.

To restore your saved ZoneAlarm security settings:

1. From the **Tools** menu, choose **Preferences**.
2. In the Backup and Restore area, click Restore.
3. Select the XML file which contains the settings you want to use.
4. Click Open.

Setting general product preferences

By default, ZoneAlarm security software starts automatically when you turn on your computer. Use the settings in the General area to change this and other options.

To set startup preferences:

1. From the **Tools** menu, select **Preferences**.
2. In the **Startup** area, select or deselect **Load ZoneAlarm security software at startup.**

To set startup preferences:

1. In the Proxy Configuration area, enter the IP address of your proxy server information only if you are certain that it is necessary to do so.

Note - ZoneAlarm security software automatically detects most proxy configurations, such as those configured through Internet Explorer. making it unnecessary to enter that information here. You should enter proxy information only if you have an uncommon proxy configuration, such as a scripted proxy, and if some product features such as anti-virus updates or instant messaging aren't working.

Setting product update options

When you purchase ZoneAlarm security software you receive a subscription for free updates to your product, which means you can receive the bug fixes, new features, and enhancements included in any updates to the product.

By default, the updates automatically sent to you. If for some reason you don't want them, you can disable the product update feature by choosing **Scheduled Tasks** from the **Tools** menu and selecting the disable option for Product Update.

Note - Product updates are different than virus signature updates. To control virus signature updates, which happen automatically and in the background, see Keeping virus definitions up-to-date (on page 122).

Licensing, registration, and support

In order to receive support and updates for ZoneAlarm security software, you need a valid license.

- When your license expires (on page 15)
- Renewing your product license (on page 16)
- Updating your ZoneAlarm registration information (on page 16)
- Accessing technical support (on page 16)

When your license expires

When your license is going to expire, ZoneAlarm will warn you.

When you purchase a ZoneAlarm product, it is yours to use forever. With the purchase you also receive one or more years of online technical support and free updates to your version of the software. These updates include product enhancements as well as important security updates to keep you protected from new threats.

Once the license expires, you can renew it to receive product updates and technical support. If you do not renew your license, the product continues to work, but is not updated to detect newly discovered malware.

Renewing your product license

When your license or trial expires, you will see messages that provide a button for renew button.

You can also renew at any time using links that appear in the lower right corner of the ZoneAlarm window. If you have been using a trial or beta license key and have just purchased a full license, you can also the enter the license key in the same manner.

After you renew your license or enter a new license, click **Update** in ZoneAlarm to update your license status in the ZoneAlarm window.

Accessing technical support

If your license subscription is current, you can access the free online technical support at http://www.zonealarm.com/support http://www.zonealarm.com/support at any time.

Updating your ZoneAlarm registration information

When you purchase ZoneAlarm security software, you are registered and can receive security news from ZoneAlarm. If your information changes, you can update it.

To update your registration information:

1. Select **Tools** | **Preferences**.
2. In the Registration area, click **Change Reg**.
3. Enter your information in the fields provided.

   To be notified of product news and updates, select the check box labeled **Inform me of important updates and news**, then click **OK**.

About updating from a prior version

When you purchase ZoneAlarm security software, you receive automatic product updates for the length of the license you purchased, which means that when a new version of your ZoneAlarm security software is released, your software notifies you and you can download it instantly for free.

You can also get the latest version by doing the following:

1. Open ZoneAlarm.
2. Click **Update** in the upper right corner.

When you update from a prior version, the installer program preserves your ZoneAlarm settings when possible.

Moving to a different computer

If you wish to move ZoneAlarm to a new machine, per the licensing agreement, completely remove it from the existing machine, and then install it on the new machine. Use the same license key that you used previously.

If you have a multi-user license, download a version on each machine or use your CD and the same license key on each machine.

Enter your ZoneAlarm license key on the new computer by clicking the prompt in the lower right corner of the ZoneAlarm window.

Uninstalling ZoneAlarm

To uninstall ZoneAlarm, use the standard method provided by your Windows operating system:

1. From the Windows **Start** menu, choose **Control Panel** | **Programs and Features** (or Add/Remove Programs).
2. Find and select ZoneAlarm from the list of programs, then select it and right-click to choose **Uninstall**.

Configuring for networks and resources

If you're on a home network, business Local Area Network (LAN), or Virtual Private Network (VPN), or a wireless network, you want to ensure smooth communication with the network while still maintaining high security. The Network Configuration Wizard, automatic VPN configuration, and other features of ZoneAlarm security software help you to quickly set up your network environment.

Configuring a new network connection

When your computer connects to a network, you can decide whether to place that network in the Trusted Zone or in the Public Zone.

ZoneAlarm helps you make this decision by determining whether a detected LAN network is public or private, secure or unsecured. It will make a default choice for you, but opens a new network dialog for you so you can confirm or change the choice.

- **Placing a network in the Trusted Zone** enables you to share files, printers, and other resources with other computers on that network. Networks you know and trust, such as your home or business LAN and known protected wireless networks, should go in the Trusted Zone.
- **Placing a network in the Public Zone** prevents you from sharing resources with other computers on that network and protects you from the security risks associated with resource sharing. Unknown networks and most wireless networks, even secured wireless networks, should go in the Public Zone.

Using the Network Configuration Wizard

When your computer connects to a new network, ZoneAlarm security software opens the Network Configuration Wizard, displaying the IP address of the detected network.

The IP address of the network is used to determine whether it is a private network or a public network.

A private network is usually a home or business Local Area Network (LAN). Private networks are placed in the Trusted Zone by default.

A public network is usually a much larger network, such as that associated with an ISP. Public networks are placed in the Public Zone by default.

To configure your network connection using the Network Configuration Wizard:

1. Choose the level of security you want for this network.
2. Optionally, if you are an advanced user, enter a name for the network if you want to be able to recognize it on the Firewall panel.

About Wireless Network Configuration

When your computer connects to a new wireless network, ZoneAlarm security software opens the Network Configuration Wizard, then displays the IP address of the detected network.

The WPA setting on the wireless access point is used to determine whether it is a *secured* wireless network or an *unsecured* wireless network.

A secured wireless network is WPA enabled. WPA provides an initial barrier that can be penetrated by hackers. In order to truly secure the network, the wireless access point must have other features implemented, such as a limited access list or SSID (Service Set Identifier) broadcast disabled. Only place wireless networks that you know have a higher level of security and where you need to share resources or print in the Trusted Zone.

An unsecured wireless network may be completely unprotected and accessible by anyone, so unsecured networks are placed in the Public Zone by default.

Integrating with network services

If you're working on a home or business network, you may want to share files, network printers, or other resources with other people on the network, or send and receive e-mail through your network's mail servers. Use the instructions in this section to enable safe resource sharing.

- Enabling file and printer sharing (on page 19)
- Connecting to network mail servers (on page 19)
- Enabling Internet Connection Sharing (on page 20)

Enabling file and printer sharing

To share printers and files with other computers on your network, you will need to configure ZoneAlarm security software to allow access to the computers with which you plan to share resources.

To configure ZoneAlarm security software for file and printer sharing:

Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone:

- Go to the **Computer | Advanced Firewall | View Zones** panel.
- Under the **Name** column, find your home network (it may be the only listing), and on that row right-click the word "Internet" under **Zone** and choose **Trusted** from the pop-up menu.

Note - If the default Trusted Zone security level has been changed, reset it to Medium. This allows trusted computers to access your shared files.

If the default Public Zone security level has been changed, reset it to High. This makes your computer invisible to non-trusted machines.

See Setting the security level for a Zone (on page 25).

Connecting to network mail servers

ZoneAlarm security software is configured to automatically work with Internet-based mail servers using POP3 and IMAP4 protocols, when you give your e-mail client permission to access the Internet.

Some mail servers, like Microsoft Exchange, include collaboration and synchronization features that might require you to trust the server in order for those services to work.

To configure ZoneAlarm security software for mail servers with collaboration and synchronization features:

1. Add the network subnet or IP address of the mail server to your Trusted Zone.

2. Set the Trusted Zone security level to Medium. This allows server collaboration features to work.
3. Set Public Zone security level to High. This makes your computer invisible to non-trusted machines.

Enabling Internet Connection Sharing

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, you can protect all of the computers that share the connection from inbound threats by installing ZoneAlarm security software on the gateway machine only. However, to receive outbound protection, or to see alerts on the client machines, you must have ZoneAlarm security software installed on the client machines as well.

Note - Before you configure ZoneAlarm security software, use your ICS software to set up the gateway and client relationships. If you use hardware such as a router to share your Internet connection rather than Microsoft's Internet Connection Sharing (ICS), ensure that the local subnet is in the Trusted Zone.

Configuring your VPN connection

ZoneAlarm security software is compatible with many types of VPN client software and can automatically configure the connection for certain VPN clients.

Supported VPN protocols

ZoneAlarm security software monitors the VPN protocols listed in the table below.

Networking Protocol	Explanation and Comments
AH	Authentication Header Protocol
ESP	Encapsulating Security Payload protocol
GRE	Generic Routing Encapsulation protocol
IKE	Internet Key Exchange protocol
IPSec	IP Security protocol.

Networking Protocol	Explanation and Comments
L2TP	Layer 2 Tunneling protocol. L2TP is a more secure variation of PPTP.
LDAP	Lightweight Directory Access protocol
PPTP	Point-to-Point Tunneling protocol
SKIP	Simple Key Management for Internet Protocol

Supported VPN protocols

Configuring your VPN connection automatically

When VPN traffic is detected, an Automatic VPN Configuration alert is displayed. Depending upon the type of VPN activity detected, and whether ZoneAlarm security software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

For detailed information about the types of Automatic VPN Configuration alerts you may see and how to respond to them, see Automatic VPN Configuration alert (on page 81).

For instance, manual action may be required if the loopback adaptor or the IP address of the VPN gateway falls within a range or subnet that you have blocked. For more information, see Configuring your VPN connection manually (on page 21).

Note - If you have created an expert firewall rule that blocks VPN traffic, you will need to modify the expert rule to allow VPN traffic. See Creating expert firewall rules (on page 36).

Configuring your VPN connection manually

If your VPN connection cannot be configured automatically, ZoneAlarm security software displays a Manual Action Required alert informing you of the manual changes you need to make to configure your connection.

Refer to the following sections for manual configuration instructions:

- Adding a VPN gateway and other resources to the Trusted Zone (on page 22)
- Removing a VPN gateway from a blocked range or subnet (on page 23)
- Allowing VPN protocols (on page 23)

- Granting access permission to VPN software

Note - If you have created an expert firewall rule that has blocked PPTP traffic and your VPN software uses PPTP, you will need to modify the expert rule. See Creating expert firewall rules (on page 36).

Adding a VPN gateway and other resources to the Trusted Zone

In addition to the VPN gateway, There may be other VPN-related resources that need to be in the Trusted Zone for your VPN to function properly.

Required Resources	Other Resources
The resources below are required by all VPN client computers and must be added to the Trusted Zone.	The resources below may or may not be required, depending on your specific VPN implementation.
VPN Concentrator	DNS servers
Remote host computers connected to the VPN client (if not included in the subnet definitions for the corporate network)	Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host.
Corporate Wide Area Network (WAN) subnets that will be accessed by the VPN client computer	Internet Gateway
Corporate LANs that will be accessed by the VPN computer	Local subnets
	Security servers (for example, RADIUS,ACE, or TACACS servers)

Required VPN-related network resources

See Adding to the Trusted Zone (on page 30) to learn how to add resources to your computer's Trusted Zone.

Removing a VPN gateway from a blocked range or subnet

If the VPN gateway falls within a range or subnet that you have blocked, you must manually unblock the range.

To unblock an IP range or subnet:

1. Select **COMPUTER | Advanced Firewall| Settings.**
2. Click **View Zones**, and in the Zone column, select the blocked IP range or subnet.
3. Select **Trusted** from the shortcut menu, then click **Apply**.

Allowing VPN protocols

To ensure proper configuration of your VPN software with ZoneAlarm security software, you will need to modify your general security settings to allow VPN protocols.

To allow VPN protocols:

1. Select **COMPUTER | Advanced Firewall** | **Settings | Advanced Settings.**
2. In the General settings area, select the check box labeled **Allow VPN protocols**.
3. Click **OK**.

Note - If your VPN program uses protocols other than GRE, ESP, and AH, also select the check box labeled **Allow uncommon protocols at high security**.

Granting access permission to VPN software

Grant access permission to the VPN client and any other VPN-related programs.

To grant permission to your VPN program:

1. Select **Application Control**| **View Programs**.
2. In the Programs column, select your VPN program.
3. In the Inbound and Outbound columns, click the "X's" and select **Allow** from the shortcut menu.

Note - If your VPN program is not listed, click **Add** to add it to the list.

To grant access to VPN-related components:

1. Select **Application Control**| **View Components**.

2. In the Components column, select the VPN component for which you want to grant access.
3. In the Inbound and Outbound columns, click the"X's" and select **Allow** from the shortcut menu.

If you are experiencing problems with your VPN connection, refer to the VPN troubleshooting tips in Troubleshooting ("Troubleshooting VPN problems" on page 170).

Firewall protection

Firewall protection is your front line of defense against Internet threats. ZoneAlarm security software's default Zones and security levels give you immediate protection against the vast majority of threats. If you're an advanced user, custom port permissions and expert rules give you detailed control of traffic based on source, destination, port, protocol, and other factors.

Understanding Firewall protection

In buildings, a firewall is a barrier that prevents a fire from spreading. In computers, the concept is similar. There are a variety of "fires" out there on the Internet—hacker activity, viruses, worms, and so forth. A firewall is a system that stops these attempts to damage your computer.

The ZoneAlarm security software firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. ZoneAlarm security software examines all the network traffic arriving at your computer, and asks these questions:

- What Zone did the traffic come from and what port is it addressed to?
- Do the rules for that Zone allow traffic through that port?
- Does the traffic violate any global rules?
- Is the traffic authorized by a program on your computer (Application Control settings)?

The answers to these questions determine whether the traffic is allowed or blocked.

- Choosing security levels (on page 25)
- Setting advanced security options (on page 26)
- Managing traffic sources (on page 29)
- Blocking and unblocking ports (on page 32)
- Understanding expert firewall rules (on page 35)

Choosing security levels

The default firewall *security levels* (High for the Public Zone, Med. for the Trusted Zone) protect you from hacker activity (such as a *port scan*), while enabling you to share printers, files, and other resources with trusted computers on your local network. In most cases, you don't have to make any adjustment to these defaults. You're protected as soon as ZoneAlarm security software is installed!

- Setting the security level for a Zone (on page 25)
- Setting advanced security options (on page 26)

Setting the security level for a Zone

Security levels make it easy to configure your firewall settings. You can apply a preconfigured security level (High, Medium, or Off) to each Zone, or you can specify the port and protocol restrictions for each level. See Blocking and unblocking ports (on page 32).

To set the security level for a Zone:

1. Select **COMPUTER | Advanced Firewall**.
2. In the Public Zone Security area, click the slider and drag it to the desired setting.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows *NetBIOS (Network Basic Input/Output System)* services, file and printer shares **is blocked**. Ports are blocked unless you have provided permission for a program to use them.
Med	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.

3. In the Trusted Zone Security area, click the slider and drag it to the desired area.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows (NetBIOS) services, file and printer shares **is blocked**. Ports are blocked unless you have provided permission for a program to use them.

Med	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.

Setting advanced security options

Advanced security options enable you to configure the firewall for a variety of special situations, such as gateway enforcement and Internet Connection Sharing (ICS).

- Setting gateway security options
- Setting ICS (Internet Connection Sharing) options
- Setting general security options (on page 26)
- Setting network security options (on page 27)

Setting general security options

These controls apply global rules regarding certain protocols, packet types and other forms of traffic (such as server traffic) to both the Trusted Zone and the Public Zone.

To modify general security settings:

1. Select **COMPUTER | Advanced Firewall** and click **Advanced Settings**.
2. In the General area, choose your security settings.

Block all fragments	Blocks all incomplete (fragmented) IP data packets. Hackers sometimes create fragmented packets to bypass or disrupt network devices that read packet headers. **Caution**: If you select this option, ZoneAlarm security software will silently block all fragmented packets without alerting you or creating a log entry. Do not select this option unless you are aware of how your online connection handles fragmented packets.
Block trusted servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.

Block Internet servers	Prevents all programs on your computer from acting as servers to the Public Zone. Note that this setting overrides permissions granted in the Programs panel.
Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target computer. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.
Allow VPN Protocols	Allows the use of VPN protocols (ESP, AH, GRE, SKIP) even when High security is applied. With this option disabled, these protocols are allowed only at Medium security.
Allow uncommon protocols at high security	Allows the use of protocols other than ESP, AH, GRE, and SKIP, at High security.
Lock hosts file	Prevents your computer's hosts file from being modified by hackers through sprayer or Trojan horses. Because some legitimate programs need to modify your hosts file in order to function, this option is turned off by default.
Disable Windows Firewall	Detects and disables Windows Firewall.
Filter IP over *1394* traffic	Filters FireWire traffic. You will need to restart your PC for these filter changes to take effect.

3. Click **OK**.

Note - ZoneAlarm filters Internet Protocol version 6 (IPv6) traffic by default. When the ZoneAlarm firewall is set to block IPv6, it also tells Windows not to use it, so you will see IPv6 disabled in your network settings.

Setting network security options

Automatic network detection helps you configure your Trusted Zone easily so that traditional local network activities such as file and printer sharing aren't interrupted. ZoneAlarm security software detects only networks that you are physically connected to. Routed or virtual network connections are not detected.

You can have ZoneAlarm security software silently include every detected network in the Trusted Zone; or ask you in each case whether to add a newly detected network.

To specify Network settings:

1. Select **Computer | Advanced Firewall** and click the **Advanced Settings** button..
2. In the Network settings area, choose your security settings.

Include networks in the Trusted Zone upon detection	Automatically moves new networks into the Trusted Zone. This setting provides the least security.
Exclude networks from the Trusted Zone upon detection	Automatically blocks new networks from being added to the Trusted Zone and places them in the Public Zone. This setting provides the most security.
Ask which Zone to place new networks in upon detection	ZoneAlarm security software displays a New Network alert or the Network Configuration Wizard, which give you the opportunity to specify the Zone.
Automatically put new unprotected wireless networks (WEP or WPA) in the Public Zone	Puts unsecured wireless networks into the Public Zone automatically, which prevents unauthorized access to your data from others accessing the network.

3. Click **OK**.

For more information about networking, see Configuring for networks and resources. ("Configuring for networks and resources" on page 17)

Setting wireless network security options

Automatic wireless network detection helps you configure your Public Zone to ensure that you computer remains secure without being interrupted each time a new network is detected.

ZoneAlarm security software detects only networks that your computer is connected to. (Networks that you are not actually connected to may appear as available networks in your network neighborhood but the New Wireless Network Configuration Wizard only appears when you connect establish a connection to that network.)

You can have ZoneAlarm security software silently include every detected wireless network in the Public Zone.

To specify Network settings:

1. Select **COMPUTER | Advanced Firewall**.
2. Click **Advanced Settings** button.
3. In the Wireless Network settings area, choose your security settings.

Automatically put new unprotected wireless networks (WEP or WPA) in the Public Zone	ZoneAlarm security software places new wireless networks in the Public Zone when they are detected.

4. Click **OK**.

For more information about networking, see Configuring for networks and resources (on page 17).

Managing traffic sources

The Zones panel contains the traffic sources (computers, networks, or sites) you have added to the Trusted Zone or Blocked Zone. It also contains any networks that ZoneAlarm security software has detected. If you are using a single, non-networked PC, the traffic source list displays only your ISP's (Internet Service Provider's) network, which should be in the Public Zone.

- Viewing the traffic source list (on page 29)
- Modifying traffic sources (on page 30)
- Adding to the Trusted Zone (on page 30)
- Adding to the Blocked Zone (on page 31)
- Viewing logged Firewall events

Viewing the traffic source list

The traffic source list displays the traffic sources and the Zones they belong to. You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

Field	Description
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source
Entry Type	The type of traffic source: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked

Traffic source list fields

Modifying traffic sources

From the traffic source list, you can move the traffic source from one Zone to another, add, edit, or remove a traffic source.

To change the Zone of a traffic source:

1. Select **COMPUTER | Advanced Firewall| Settings | View Zones.**
2. Locate the traffic source, then click in the **Zone** column.
3. Select a Zone from the shortcut menu, then click **Apply**.

To add, remove, or edit a traffic source:

1. Select **COMPUTER | Advanced Firewall| Settings | View Zones.**
2. In the Name column, click the traffic source, then click **Add**, **Edit**, or **Remove**.
3. Click **Apply**.

Adding to the Trusted Zone

The Trusted Zone contains computers you trust and want to share resources with. For example, if you have three home PCs that are linked together in an Ethernet network, you can put each individual computer or the entire network adapter subnet in the Trusted Zone. The Trusted Zone's default medium security settings enable you to safely share files, printers, and other resources over the home network. Hackers are confined to the Public Zone, where high security settings keep you safe.

Note - The easiest way to add something to the Trusted Zone is to go to **Tools | Logs | Log Viewer and** see if the IP address, network, host, or site has shown up in the logs. Right-click it and choose **Add to Zone** | **Trusted**.

To add a single IP address:

1. Select **COMPUTER | Advanced Firewall| Settings | View Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.
   The Add IP Address dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address and a description in the boxes provided, then click **OK.**

To add an IP range:

1. Select **COMPUTER** | **Advanced Firewall| View Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.
   The Add IP Range dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the beginning IP address in the first field, and the ending IP address in the second field.
5. Type a description in the field provided, then click **OK**.

To add a subnet:

1. Select **COMPUTER** | **Advanced Firewall**| **View Zones**.
2. Click **Add**, then select **Subnet** from the shortcut menu.
   The Add Subnet dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address in the first field, and the Subnet mask in the second field.
5. Type a description in the field provided, then click **OK**.

To add to a Host or Site to the trusted Zone:

1. Select **COMPUTER** | **Advanced Firewall**| **View Zones**.
2. Click **Add**, then select **Host/Site**.
   The Add Host/Site dialog appears.
3. Select **Trusted** from the Zones drop-down list.
4. Type the fully qualified host name in the **Host name** field.
5. Type a description of the host/site, then click **OK**.

To add a network to the Trusted Zone:

1. Select **COMPUTER** | **Advanced Firewall**| **View Zones**.
2. In the Zone column, click the row containing the network, then select **Trusted** from the shortcut menu.
3. Click **Apply**.

Note - ZoneAlarm security software automatically detects new network connections and helps you add them to the right Zone. For more information, see Configuring for networks and resources (on page 17).

Adding to the Blocked Zone

To add to the Blocked Zone, follow the instructions for adding to the Trusted Zone, but select **Blocked** from the drop-down list in step 2.

Viewing logged Firewall events

By default, all Firewall events are recorded in the Log Viewer.

To view logged firewall events:

1. Select **Tools | Logs| Log Viewer**.

2. Select **Firewall**, from the Alert Type drop-down list.

The following table provides an explanation of the log viewer fields available for Firewall events.

Field	Information
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Date/Time	The date and time the alert occurred.
Protocol	The communications protocol used by the traffic that caused the alert.
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm security software blocked.
Destination IP	The address of the computer the blocked traffic was sent to.
Direction	The direction of the blocked traffic. "Incoming" means the traffic was sent to your computer. "Outgoing" means the traffic was sent from your computer.
Action Taken	How the traffic was handled by ZoneAlarm security software.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Source DNS	The domain name of the sender of the traffic that caused the alert.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.

Firewall event log fields

Blocking and unblocking ports

ZoneAlarm security software's default security levels determine which ports and protocols are allowed and which are blocked. If you are an advanced user, you can change the definition of the security levels by changing port permissions and adding custom ports.

- Default port permission settings (on page 33)
- Adding custom ports (on page 33)

Adding custom ports

You can allow communication through additional ports at High security, or block additional ports at Medium security by specifying individual port numbers or port ranges.

To specify additional ports:

1. Select **Firewall**.
2. In either the Trusted Zone or Public Zone area, click **Custom**.

   The Firewall settings dialog appears.
3. Scroll to the security level (High or Medium) to which you want to add ports.
4. Select the desired port type: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP.
5. Type the port or port ranges you want to allow or block in the Ports field, separated by commas. For example, 139, 200-300
6. Click **Apply**, then click **OK**.

Default port permission settings

The default configuration for High security blocks all inbound and outbound traffic through ports not being used by programs you have given access or server permission except:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67) - on Windows 9x systems
- Outgoing DNS (port 53) - If the computer is configured as an ICS gateway

Traffic Type	Security levels		
	HIGH	MED	OFF
DNS outgoing	block	n/a	allow
DHCP outgoing	block	n/a	allow
broadcast/multicast	allow	allow	allow
ICMP			
incoming (ping echo)	block	allow	allow
incoming (other)	block	allow	allow

	Security levels		
outgoing (ping echo)	block	allow	allow
outgoing (other)	block	allow	allow
IGMP			
incoming	block	allow	allow
outgoing	block	allow	allow
NetBIOS			
incoming	n/a	block	allow
outgoing	n/a	allow	allow
UDP **(ports not in use by a permitted program)**			
incoming	block	allow	allow
outgoing	block	allow	allow
TCP **(ports not in use by a permitted program)**			
incoming	block	allow	allow
outgoing	block	allow	allow

Default access permissions for incoming and outgoing traffic types

To change a port's access permission:

1. Select **COMPUTER | Advanced Firewall**.
2. In either the Public Zone or the Trusted Zone area, click **Custom**.
   The Custom Firewall Settings dialog appears.
3. Scroll to locate High and Medium security settings.
4. To block or to allow a specific port or protocol, click the check box beside it.

Important - Be aware that when you select a traffic type in the High security settings list, you are choosing to ALLOW that traffic type to enter your computer under High security, thus decreasing the protection of the High security level. Conversely, when you select a traffic type in the Medium security settings list, you are choosing to BLOCK that traffic type under Medium security, thus increasing the protection of the Med security level.

5. Click **Apply**, then click **OK**.

Understanding expert firewall rules

Expert firewall rules are intended for users experienced with firewall security and networking protocols.

Expert rules do not take the place of other rules. They are an integral part of the multiple layer security approach and work in addition to other firewall rules.

Expert rules use four attributes to filter packets:

- Source and/or destination IP address
- Source and/or destination port number
- Network protocol/message type
- Day and Time

Source and destination addresses can be specified in a number of formats, including a single IP network address, a range of IP addresses, a subnet description, a gateway address, or a domain name.

Source and destination ports are used only for network protocols that use ports, such as UDP and TCP/IP. ICMP and IGMP messages, for example, do not use the port information.

Network protocols can be selected from a list of common IP or VPN protocols, or specified as an IP protocol number. For ICMP, the message type can also be specified.

Day and Time ranges can be applied to a rule to restrict access based on the day of the week and the time of day.

- How expert firewall rules are enforced (on page 35)
- Expert firewall rule enforcement rank (on page 36)
- Creating expert firewall rules (on page 36)
- Creating groups (on page 39)
- Editing and re-ranking rules (on page 46)

How expert firewall rules are enforced

It is important to understand how expert rules are enforced in combination with Zone rules, program permissions, and other expert rules.

Expert rules and Zone rules

Expert firewall rules are enforced before Zone firewall rules. That is, if a packet matches an expert rule, that rule is enforced, and ZoneAlarm security software skips evaluation of Zone rules.

Example: Imagine you have your Trusted Zone security level set to Medium. This allows outgoing NetBIOS traffic. However, you have also created an expert rule that blocks all NetBIOS traffic

between the hours of 5PM and 7AM. Any outbound NetBIOS traffic during those hours will be blocked, in spite of the Trusted Zone setting.

Expert firewall rules and program permissions

Expert rules and Zone rules together are enforced in tandem with Program permissions. That is, if either your program permissions or Zone rules/expert firewall rules determine that traffic should be blocked, it is blocked. Note that this means that you can use firewall rules to override or redefine program permissions.

Note - Note that packets coming from the Blocked Zone will not be blocked if they are allowed by an Expert Firewall Rule.

Expert firewall rule enforcement rank

Within the realm of firewall rules, rule evaluation order becomes a factor. ZoneAlarm security software first checks expert firewall rules. If a match is found and a rule is enforced, the communication is marked as either blocked or allowed, and ZoneAlarm security software skips evaluation of Zone rules.

If no expert firewall rule is matched, ZoneAlarm security software checks Zone rules to see if the communication should be blocked.

The enforcement rank of expert firewall rules is also important. Each rule has a unique rank number, and rules are evaluated in order of rank. Only the first rule that matches is executed.

Example:

Rule 1 allows FTP clients in the Trusted Zone to connect to an FTP server on port 21. Rule 2 blocks all FTP clients from connecting on port 21, regardless of Zone. These two rules together allow clients in the Trusted Zone to use an FTP server on the client computer, but block all other FTP access.

If the order of the rules were reversed, Rule 2 would match first, and all FTP access would be blocked. Rule 1 would never have a chance to execute, so the FTP clients in the Trusted Zone would still be blocked.

Creating expert firewall rules

Creating expert firewall rules involves specifying the source or destination of the network traffic to which the rule applies, setting tracking options, and specifying the action of the rule: whether to block or to allow traffic that meets the specifications of the rule. You can create new rules from scratch, or you can copy an existing rule and modify its properties.

To create a new expert firewall rule:

1. Select **COMPUTER | Advanced Firewall| Settings | Expert Rules**, then click **Add**.

The Add rule dialog appears.

2. In the General area, specify the rule settings.

Rank	The order in which rules will be enforced. A rule with a rank of 1 is enforced first.
Name	Provide a descriptive name for the rule.
State	Specify whether the rule is enabled or disabled.
Action	Indicates whether to block or allow traffic that matches this rule.
Track	Indicates whether to log, alert and log, or do nothing when the expert rule is enforced.
Comments	Optional field for entering notes about the expert rule.

3. In the Source area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu. You can add any number of sources to a rule.

My Computer	Applies the expert rule to traffic originating on your computer.
Trusted Zone	Applies the expert rule to network traffic from sources in your Trusted Zone.
Public Zone	Applies the expert rule to network traffic from sources in your Public Zone.
All	Applies the expert rule to network traffic coming from any source.
Host/Site	Applies the expert rule to network traffic coming from specified domain name.
IP Address	Applies the expert rule to network traffic coming from specified IP address.
IP Range	Applies the expert rule to network traffic coming from a computer within the specified IP range.
Subnet	Applies the expert rule to network traffic coming from a computer within the specified subnet.
Gateway	Applies the expert rule to network traffic coming from a computer on the specified gateway.
New Group	Choose this option, then click **Add** to create a new location group to apply to the expert rule.

Existing Group	Choose this option to select one or more location groups to apply to the expert rule, then click **OK**.

4. In the Destination area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu.

   Available location types are the same for Source and Destination locations.

5. In the Protocol area, select a protocol from the list, or click **Modify**, then select **Add Protocol**.

Add Protocol	Choose this option to add a protocol to the rule. Specify: TCP, UDP, TCP + UDP, ICMP, IGMP, or Custom and refer to Step 5 of Creating a protocol group (on page 40) for help with this dialog.
New Group	Choose this option, then click **Add** to create a new protocol group to apply to the expert rule. See Creating a protocol group (on page 40) for help with this dialog.
Existing Group	Choose this option to select one or more protocol groups to apply to the expert rule, then click **OK**.

6. In the Time area, select a time from the list, or click **Modify**, then select **Add Time**.

Day/Time Range	Choose this option to add a day/time range to the rule. Specify a description, time range and one or more days. Time range is specified using a 24 hour clock.
New Group	Choose this option, then click **Add** to create a new day/time group to apply to the expert rule.
Existing Group	Choose this option to select one or more day/time groups to apply to the expert rule, then click **OK**.

7. Click **OK**.

To create a new rule from an existing rule:

1. Select **Firewall|Expert**.
2. Select the expert firewall rule you want to duplicate, then either press **Ctrl**+**C** or right-click the rule and choose **Copy**.
3. Paste the copied rule either by pressing **Ctrl**+**V**, or by right-clicking and choosing **Paste**.

Note - If a rule is currently selected in the list, the pasted rule will be inserted above the selected rule. If no rule is selected, the pasted rule will be inserted at the top of the rules list.

A "1" is appended to the name of the copied rule. If you paste a rule a second time, the number 2 is appended to the second rule copied.

4. Click **Apply** to save your changes.
5. Right-click the new rule and choose **Edit** to modify the rule properties as necessary.

Creating groups

Use groups to simplify the management of locations, protocols, and days/times that you use in your expert firewall rules.

- Creating a location group (on page 39)
- Creating a protocol group (on page 40)
- Creating a day/time group (on page 43)

Creating a location group

Use location groups to combine non-contiguous IP addresses and ranges, or different types of locations (for example, subnets and hosts), into an easily manageable set. You can then easily add that set of locations to any expert firewall rule.

Note - Once created, the names of groups cannot be changed. For example, if you create a Location Group named "Home" and subsequently decide to call the group "Work", you would need to remove the group called "Home" and create a new group with the name "Work."

To create a location group:

1. Select **COMPUTER | Advanced Firewall | Settings | Expert Rules Rules**, then click **Groups**.

   The Group Manager dialog appears.
2. Select **Locations**, then click **Add**.

   The Add Location Group dialog appears.
3. Specify the name and description of the location group, then click **Add** and select a Location type from the menu.

Host/Site	A description and host name of the Host/Site location, then click **OK**. Do not include http:// in the host name. Click **Lookup** to preview the site's IP address.
IP Address	A description and IP address of the IP Address location, then click **OK**.
IP Range	A description and beginning IP address and ending IP address of the IP Range location, then click **OK**.
Subnet	Specify a description, IP address, and Subnet Mask of the Subnet location, then click **OK**.
Gateway	Specify an IP address, MAC Address, and description of the Gateway

	location, then click **OK**.

4. Click **OK** to close the Group Manager dialog box.

Creating a protocol group

Create a protocol group to combine well-known TCP/UDP ports, protocols, and protocol-specific message types (for example, ICMP message types), into sets that you can easily add to expert rules. For example, you might create a group including POP3 and IMAP4 protocols in order to simplify the administration of your rules regarding e-mail traffic.

To create a Protocol group:

1. Select **COMPUTER | Advanced Firewall | Settings | Expert Rules Rules**, then click **Groups**.
   The Group Manager dialog appears.
2. Select **Protocols**, then click **Add**.
   The Add Protocol Group dialog appears.
3. Specify the name and description of the Protocols group, then click **Add**.
   The Add Protocol dialog appears.
4. Select a protocol type from the **Protocol** drop-down list
5. Depending on the protocol type you chose, do one of the following:
   If you chose **TCP**, **UDP**, or **TCP/UDP**, specify a destination, source and port number.

Name	Port number
FTP	21
Telnet	23
POP3	110
NNTP	119
NetBIOS Name	137
NetBIOS Datagram	138
NetBIOS Session	139
IMAP4	143
HTTPS	443
RTSP	554

Windows Media	1755
AOL	5190
Real Networks	7070
Other	Specify port number
FTP Data	20
TFTP	69
HTTP	80
DHCP	67
DHCP Client	68
SMTP	25
DNS	53

If you chose ICMP in step 4, specify a description, message name, and type number.

Message name	**Type number**
Source Quench	4
Redirect	5
Alt	6
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time Exceeded	11
Parameter Problem	12
Timestamp	13
Timestamp reply	14

Information request	15
Information reply	16
Address Mask Request	17
Address Mask Reply	18
Traceroute	30
Other	Specify type number

If you chose **IGMP,** specify a description, message name, and type number.

Membership Query	17
Membership Report (ver 1)	18
Cisco Trace	21
Membership Report (ver 2)	22
Leave Group (ver 2)	23
Multicast Traceroute Response	30
Multicast Traceroute	31
Membership Report (ver 3)	34
Other	Specify type number.

If you chose **Custom**, specify a description, protocol type, and protocol number.

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57

Other	Specify protocol number.

6. Click **OK**, to close the Add Protocol dialog.

Creating a day/time group

To allow or block network traffic to or from your computer during specified periods of time, you can create a day/time group and then add it to an expert rule. For example, to block traffic coming from pop-up ad servers during business hours, you could create a group that blocks HTTP traffic coming from a specified domain during the hours of 9 AM and 5 PM, Monday through Friday.

To create a Day/Time group:

1. Select **COMPUTER | Advanced Firewall**| **Expert Rules**, then click **Groups**.
   The Group Manager dialog appears.
2. Select **Times**, then click **Add**.
   The Add Time Group dialog appears.
3. Specify the name and description of the Time group, then click **Add**.
   The Add Time dialog appears.
4. Specify a description of the time, then select a time and day range.
5. Click **OK**, then click **OK** to close the Group Manager.

Managing Expert Firewall Rules

From the **COMPUTER | Advanced Firewall | Settings | Expert Rules** panel, you can view the status of existing expert rules, enable or disable rules, edit or remove rules, add new rules, change the order of rules, and create groups.

- Understanding expert firewall rules (on page 35)
- Creating expert firewall rules (on page 36)
- Editing and re-ranking rules (on page 46)
- Viewing the Expert Rules list (on page 43)
- Editing and re-ranking rules (on page 46)

Viewing the Expert Rules list

The Expert Rules panel presents a list of all expert firewall rules. Rules are listed in order of enforcement priority (rank). The arrow buttons on the right-hand side more selected rules up and down the list, changing the enforcement order of the selected rules.

You also can change rank order of rules by dragging and dropping rules from one position to another.

For example, dragging and dropping rule 2 to the top of the list changes the rank of that rule to 1.

Rank

The enforcement priority of the rule. Rules are evaluated in order of rank, starting with number 1, and the first rule that matches will be enforced. Disabled rules will display "Off" instead of a rank number, but will retain their rank ordering in the list.

Action

The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.

- **Block** - The traffic is blocked.
- **Allow**- The traffic is allowed.

In rules with access roles, you can add a property in the **Action** field to redirect traffic to the Captive Portal. If this property is added, when the source identity is unknown and traffic is HTTP, the user is redirected to the Captive Portal. If the source identity is known, the **Action** in the rule (Allow or Block) is enforced immediately and the user is not sent to the Captive Portal. After the system gets the credentials from the Captive Portal, it can examine the rule for the next connection.

To redirect HTTP traffic to the Captive Portal:

1. In a rule that uses an access role in the **Source** column, right-click the **Action** column and select **Edit Properties**.

   The Action Properties window opens.
2. Select **Redirect HTTP connections**.
3. Click **OK**.

   The Action column shows that a redirect to the Captive Portal occurs.

Track

Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Click in the column and the options open. The options include:

- **None** - Does not record the event
- Logs:
  - **Log** - Records the event's details in SmartView Tracker. This option is useful for obtaining general information on your network's traffic. There is one log for each session. It shows one URL and one or more suppressed logs.
  - **Extended Log** - Consolidates logs by session (shows the number of suppressed logs) and includes data for each URL connection in the session time frame. Each of the URLs has an entry in the URLs tab in SmartView Tracker. Using this option can have an affect on performance.
  - **Complete Log** - Records events for each URL request made regardless of session. Each URL connection has its own log.

- **Account** - Records the event in SmartView Tracker with byte information
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **SNMP Trap** - Sends a SNMP alert to the SNMP GUI, or runs the script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in **Policy > Global Properties > Log and Alert > Alert Commands**

Name

Give the rule a descriptive name. The name can include spaces.

Double-click in the **Name** column of the rule to add or change a name.

Source

The source is where the traffic originates. The default is **Any**.

Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple sources. The source can be an Access Role object, which you can define when Identity Awareness is enabled.

Destination

Choose the destination for the traffic. The default is the **Internet**, which includes all traffic with the destination of DMZ or external.

To choose other destinations, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple destinations.

Protocol

The network protocol to which the rule applies.

Time

The time period during which the rule is active.

Editing and re-ranking rules

You can edit or reorder existing expert rule from the Expert Rules list by selecting rules and dragging them into the desired rank. Note that if you have copied an expert rule into the rules for a Program, changing the expert rule does not automatically change the Program rule. For more information, see Creating expert rules for programs.

To edit a rule:

1. Select **COMPUTER | Advanced Firewall| Settings | Expert Rules.**
2. Select the rule you want to edit, then click **Edit**.
   The Edit Rule dialog appears.
3. Modify rule attributes as necessary, then click **OK**.

To change the rank of a rule:

1. Right-click the rule you want to move, then select **Move Rule**.

Move to Top	Moves the selected rule to the top of the Rules list.
Move to Bottom	Moves the selected rule to the bottom of the Rules list.
Move Up	Moves the selected rule one row up in the Rules list.
Move Down	Moves the selected rule one row down in the Rules list.

Understanding and reducing alerts

There are many different types of security alerts that you might see while ZoneAlarm security software is protecting you. Here is where you find out why certain alerts happen, what they mean, and what to do about them. You will also find tips for reducing the number of alerts you see.

Note: For information about suppressing most alerts while playing games on your computer, see Game Mode (on page 168).

About alerts and managing them

ZoneAlarm security software alerts fall into three basic categories: informational, program, and network. Additional alerts that may appear if the your version of the product includes ID Lock alerts and OSFirewall alerts.

You can specify:

- Whether you want to be alerted to all security and program events, or if you only want to be notified of events that are likely a result of hacker activity.
- Whether you want to see all alerts or only High-rated alerts. (Although some Program and ID Lock alerts cannot be suppressed as they need you to decide whether to grant permission.)

  You can also configure and monitor logs of alerts. For information about making any of these general or log settings, see Managing Alerts and Logs (on page 159).
-

Informational alerts

Informational alerts tell you that ZoneAlarm security software has blocked a communication that did not fit your security settings. They do not require a decision from you.

- Firewall alerts/Protected (on page 47)
- MailSafe alert (on page 50)
- Blocked Program alert (on page 53)
- Internet Lock alert (on page 56)
- Remote alert (on page 59)

Firewall alerts/Protected

Firewall alerts are the most common type of informational alert. Firewall alerts inform you that the ZoneAlarm security software firewall has blocked traffic based on port and protocol restrictions or other firewall rules.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe

to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.

Detected Behavior	What this means	Recommendation
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security	A program is trying to modify the Telecom Italia	Unless you are upgrading the Telecom Italia security software

Detected Behavior	What this means	Recommendation
software program	security software program, possibly to prevent it from running, or performing product updates.	client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

MailSafe alert

MailSafe alerts let you know that ZoneAlarm security software has quarantined a potentially dangerous attachment to an e-mail message.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse	A program is attempting to remotely control your	Unless you are running remote-access software, such as

Detected Behavior	What this means	Recommendation
input	keyboard and mouse.	PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.

Detected Behavior	What this means	Recommendation
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Blocked Program alert

Blocked Program alerts tell you that ZoneAlarm security software has prevented an application on your computer from accessing the Internet or Trusted Zone resources. By clicking OK, you're not allowing the program access, just acknowledging that you saw the alert.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with

information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.

Detected Behavior	What this means	Recommendation
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other

Detected Behavior	What this means	Recommendation
		cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Internet Lock alert

Internet Lock alerts let you know that ZoneAlarm security software has blocked incoming or outgoing traffic because the Internet Lock (or the Stop button) is engaged. By clicking OK, you're not opening the lock; you're just acknowledging that you've seen the alert.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts. See Firewall zone basics (on page 9).

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard	A program is attempting	Unless you are running a

Detected Behavior	What this means	Recommendation
and mouse input	to monitor your keyboard strokes and mouse input.	specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set

Detected Behavior	What this means	Recommendation
		to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Remote alert

Remote alerts are displayed on an ICS client machine when ZoneAlarm security software blocked traffic at the ICS gateway. If you are not on a machine that is a client in an ICS network, you will never see this alert.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP’s network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard	A program is attempting	Unless you are running a

Detected Behavior	What this means	Recommendation
and mouse input	to monitor your keyboard strokes and mouse input.	specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set

Detected Behavior	What this means	Recommendation
		to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Program alerts

Application control, which generates program alerts, is the most important part of your strong outbound protection system.

Program alerts sometimes appear to ask you to give permssions to a legitimate program that ZoneAlarm doesn't yet know.

They can also protect you if, for example, a Trojan horse virus or worm on your computer is trying to spread, or if a program on your computer is trying to modify your operating system.

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server.

Some basics on responding to program alerts:

- By clicking **Allow**, you grant permission to the program.
- By clicking **Deny**, you deny permission to the program.

See the topics below for more explanation and helpful tips about responding to and reducing each kind of program alert.

How do you know which type of program alert you are seeing on your system? Look at the name at the top of the program alert message.

- New Program alert (on page 63)
- Repeat Program alert (on page 66)
- Changed Program alert (on page 69)
- Program Component alert
- Server Program alert (on page 75)
- Advanced Program alert (on page 78)
- Automatic VPN Configuration alert (on page 81)
- Manual Action Required alert (on page 85)

New Program alert

New Program alerts enable you to set access permission for program that has not asked for Public Zone or Trusted Zone access before. If you click Allow, the program is allowed access. If you click Deny, the program is denied access.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe

to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.

Detected Behavior	What this means	Recommendation
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security	A program is trying to modify the Telecom Italia	Unless you are upgrading the Telecom Italia security software

Detected Behavior	What this means	Recommendation
software program	security software program, possibly to prevent it from running, or performing product updates.	client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Repeat Program alert

Repeat Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Public Zone or Trusted Zone, and that program has asked for permission before.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse	A program is attempting to remotely control your	Unless you are running remote-access software, such as

Detected Behavior	What this means	Recommendation
input	keyboard and mouse.	PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.

Detected Behavior	What this means	Recommendation
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Changed Program alert

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow. If you click Allow, the changed program is allowed access. If you click Deny, the program is denied access.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with

information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.

Detected Behavior	What this means	Recommendation
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other

Detected Behavior	What this means	Recommendation
		cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Program Component alert

Use the Program Component alert to allow or deny Internet access to a program that is using one or more components that haven't yet been secured by ZoneAlarm security software. This helps protect you from hackers who try to use altered or faked components to get around your Application Control restrictions.

By clicking Allow, you allow the program to access the Internet while using the new or changed components. By clicking Deny, you prevent the program from accessing the Internet while using those components.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP’s network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard	A program is attempting	Unless you are running a

Detected Behavior	What this means	Recommendation
and mouse input	to monitor your keyboard strokes and mouse input.	specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set

Detected Behavior	What this means	Recommendation
		to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Server Program alert

Server Program alerts enable you to set server permission for a program on your computer.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP’s network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard	A program is attempting	Unless you are running a

Detected Behavior	What this means	Recommendation
and mouse input	to monitor your keyboard strokes and mouse input.	specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set

Detected Behavior	What this means	Recommendation
		to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Advanced Program alert

Advanced Program alerts are similar to other Program alerts (New Program, Repeat Program, and Changed Program)—they inform you that a program is attempting to access the network.

However, they differ from other Program alerts in that the program is attempting to use another program to connect to the Internet, or is attempting to manipulate another program's functionality.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.

Detected Behavior	What this means	Recommendation
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser,

Detected Behavior	What this means	Recommendation
		or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Automatic VPN Configuration alert

Automatic VPN Configuration alerts occur when ZoneAlarm security software detects VPN activity. Depending upon the type of VPN activity detected, and whether ZoneAlarm security

software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a

Detected Behavior	What this means	Recommendation
		reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a	A program is attempting to modify another	Unless a program you are using has a reason to open another

Detected Behavior	What this means	Recommendation
good one	program.	program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Manual Action Required alert

A Manual Action Required alert informs you that further steps must be taken before ZoneAlarm security software is properly configured to support your VPN connection.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a

Detected Behavior	What this means	Recommendation
	program	program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.

Detected Behavior	What this means	Recommendation
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

OSFirewall alerts

OSFirewall alerts are alerts that appear when programs or processes on your computer are attempting to modify your computer's settings or programs.

There are three types of OSFirewall alerts, two of which require a response from you: Medium-rated Suspicious and High-rated Suspicious. Malicious alerts do not require a response from you.

- Medium-rated Suspicious Behavior alert (on page 88)
- High-rated Suspicious Behavior alert (on page 91)
- Malicious behavior alert (on page 94)

Medium-rated Suspicious Behavior alert

Medium-rated Suspicious Behavior alerts inform you that a trusted program is trying to perform an action that may change the default behavior of a program.

For example, if a program were to modify your browser's home page, you would see a Medium-rated Suspicious Behavior alert. If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is given Restricted access, which means that all future suspicious behavior will be denied.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is

Detected Behavior	What this means	Recommendation
	Internet access or to leak information.	probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.

Detected Behavior	What this means	Recommendation
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program

attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

High-rated Suspicious Behavior alert

A High-rated Suspicious Behavior alert informs you that a program on your computer is attempting activity that could be dangerous.

Examples of such behaviors include:

- attempts to access a disk without going through the file system. This behavior is used by malicious software to get around file protection by changing raw data on your disk.
- behavior that may cause programs or your operating system to stop functioning normally
- behaviors that indicates spyware is trying to monitor your activity

If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is given Restricted, access which means that all future suspicious behavior will be denied.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading	Unless you are installing anti-virus, anti-spyware, firewall,

Detected Behavior	What this means	Recommendation
	a driver allows a program to do anything it wants on your computer.	VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running,	Unless you are upgrading the Telecom Italia security software client, deny this action.

Detected Behavior	What this means	Recommendation
	or performing product updates.	

High-rated suspicious behavior guide

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

Malicious behavior alert

A Malicious Behavior alert informs you that a malicious program is attempting to run on your computer. Programs that are designated by ZoneAlarm security experts tend to be known worms, viruses, trojans, or other such malware.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.

Detected Behavior	What this means	Recommendation
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

ID Lock alert

An ID Lock alert informs you that information stored in myVAULT is about to be sent to a destination that is not on the Trusted Sites list.

If they have enabled the ID Lock feature, users may see ID Lock alerts if the personal information stored in myVAULT is sent to a destination that is not listed on their Trusted Sites list.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.

Detected Behavior	What this means	Recommendation
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program controlApplication Controling set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was canceled, it will delete the run key. In other cases, you should deny this action.
Modification of Telecom Italia security software program	A program is trying to modify the Telecom Italia security software program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the Telecom Italia security software client, deny this action.

Note-Telecom Italia security software security software will remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

Application Control

Application control helps keep bad programs on your PC from accessing the Internet while making sure that good programs have the access they need.

You can assign application control permissions manually or let ZoneAlarm security software assign permissions when program advice is available. Advanced users can control the ports that each program is permitted to use.

Understanding Application Control

Your outbound protection is called Application Control. Everything you do on the Internet—from browsing Web pages to downloading audio files—is managed by specific programs on your computer. Hackers exploit this fact by planting "malware"—malicious software—on your computer.

Malware can masquerade as harmless e-mail attachments or as updates to legitimate applications. Once on your computer, however, the malware can hijack trusted applications and carry out malicious activities under the guise of legitimacy.

ZoneAlarm security software protects your computer from hackers and malicious attacks by assigning policies to programs that indicate their level of trustworthiness and specify the actions they are allowed to perform.

Some versions of ZoneAlarm security software include OSFirewall protection, which detects when programs try to use your operating system to perform suspicious actions on your computer.

The minimum you need to know about program control

- By default, a program's permission to access the Internet is automatically determined by SmartDefense Advisor.
- Alerts appear if SmartDefense Advisor is unfamiliar with a program. (When the unknown program wants access the Internet for the first time, a **New Program alert** asks if you want to grant the access.)
- If a program is trying to *act as a server,* a **Server Program alert** asks you if you want to grant server permission. A program "acts as a server" when it is open to receive connection requests from other computers. Though some applications, such as e-mail programs, may need to act as servers to operate, hacker programs act as servers to receive instructions from their creators. Be careful to give server permission only to programs that you trust and that need server permission to operate.
- You can control the Internet and server permissions for specific programs by using the Program Control panel or by allowing program control to ask you about each program as it is activated.

Setting program permissions automatically

The SmartDefense Advisor and Application Control settings work together to ensure that good programs are given network access and that bad programs are denied access. By default, Application Control is set to Medium and SmartDefense Advisor is set to Auto. With these defaults, ZoneAlarm security software assigns permission to programs automatically. For information about customizing Application Control and SmartDefense Advisor, see Setting general Application Control options.

If SmartDefense Advisor and Application Control are set to their defaults, one of three things may occur when a program requests access for the first time:

- Access is granted - Access is granted if the program is known to be safe and requires the permissions it is asking for in order to function properly.
- Access is denied - Access is denied if the program is a known bad program or if the program does not require the permissions it is asking for.
- A New Program alert appears - Program alerts appear when you need to decide whether to allow or deny Internet access to a program. The alert may contain a recommendation about whether to allow or deny access, and, if necessary, you can click **More info** to get details about the program to help you respond.
- As long as SmartDefense Advisor is set to Auto, you see a program alert only if there is no automatic setting available. ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel. For more information about different types of Program alerts, see Program alerts (on page 62).

Safe programs

ZoneAlarm security software validates your programs against a database of known safe programs and automatically assigns the permissions required for the programs to function properly. If you accepted the default program settings in the Configuration Wizard, ZoneAlarm security software is set up to automatically configure the most popular programs in the following general categories:

- Browsers (e.g., Internet Explorer, Netscape)
- E-mail applications (e.g., Microsoft Outlook, Eudora)
- Instant Messengers (e.g., AOL, Yahoo!)
- Anti-virus (e.g., Symantec, ZoneAlarm)
- Document utilities (e.g., WinZip® and Adobe® Acrobat®)
- ZoneAlarm software applications

Even programs that are considered safe can be used by hackers to perform actions that are not. OSFirewall protection displays alerts when it detects suspicious program behavior. For more information about these alerts, see Program alerts (on page 62).

Setting program permissions manually

f you want to assign permissions to programs on your own, or if ZoneAlarm security software was unable to assign permissions automatically, you can set permissions manually by using Program alerts, or by setting permissions for specific programs on the **Application Control | View Programs** panel.

Program alerts

Application control, which generates program alerts, is the most important part of your strong outbound protection system.

Program alerts sometimes appear to ask you to give permssions to a legitimate program that ZoneAlarm doesn't yet know.

They can also protect you if, for example, a Trojan horse virus or worm on your computer is trying to spread, or if a program on your computer is trying to modify your operating system.

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server.

Some basics on responding to program alerts:

- By clicking **Allow**, you grant permission to the program.
- By clicking **Deny**, you deny permission to the program.

See the topics below for more explanation and helpful tips about responding to and reducing each kind of program alert.

How do you know which type of program alert you are seeing on your system? Look at the name at the top of the program alert message.

- New Program alert (on page 63)
- Repeat Program alert (on page 66)
- Changed Program alert (on page 69)
- Program Component alert
- Server Program alert (on page 75)
- Advanced Program alert (on page 78)
- Automatic VPN Configuration alert (on page 81)
- Manual Action Required alert (on page 85)

Programs list

The Programs list allows you to set or customize permissions for specific programs based on your individual needs. For more information about using the Programs list and customizing permissions, see Using the programs list (on page 111).

Setting general program control options

When you're using ZoneAlarm security software, no program on your computer can access the Internet or your local network, or act as a server, unless it has permission to do so.

-

Setting the program control level

ZoneAlarm security software offers several methods of program control:

- Basic program control lets you determine access and server rights for individual programs.
- The Custom Program Control Settings window provides several high-security settings that are designed to prevent malicious programs from controlling trusted programs. See Custom program control features.
- OSFirewall protection detects when programs try to use your operating system to perform suspicious actions on your computer. For details on OSFirewall, see Configuring OSFirewall protection.

Understanding Auto-Learn

Auto is the default setting for the first 21 days of using ZoneAlarm security software. ZoneAlarm security software observes and tracks which safe programs you use regularly, so that you are not interrupted with alerts about these programs. After this self-learning period, a message appears asking you whether you would like to continue in Auto learning mode or move Application Control level to Max so that you have maximum outbound protection.

To set the program control level:

1. Select **Application Control**.
2. Click the slider and drag it to the desired setting.

Max (for versions with Anti-virus) High (for versions without Anti-virus)	With this setting, you may see a large number of alerts. • Programs must ask for Internet access and server rights. • OSFirewall will monitor for suspicious behaviors, including attempts to get around file system controls by accessing raw disk data. • Advanced Program control and Application Interaction Control are enabled. • Service control manager is on if you have enabled it in the Custom program control settings. • By default, component control is disabled.*
Auto (for versions with Anti-virus)	This Auto-Learn mode minimizes alerts by recognizing your frequently used programs and giving them network access without interrupting your work with frequent alerts • This is the default level for the first 21 days. Most program alerts are suppressed by giving access to programs you frequently use and relying on SmartDefense Advisor to screen programs • The OSFirewall will also screen some programs. • Not as secure as the Max or High setting.
Medium (for versions without Anti-virus)	This is the default setting. • Programs must ask for Internet access and server rights. • OSFirewall will monitor for suspicious behaviors. • By default, component control is disabled.*
Min (for versions with Anti-virus)	• OSFirewall is disabled. • By default, component control is disabled.* • Server control and stealth mode are available
Low	• OSFirewall is disabled.

(for versions without Anti-virus)	• By default, component control is disabled.* • Server control and stealth mode are not available
Off	Program control is disabled. • No programs or components are authenticated or learned. • No program permissions are enforced. • All programs are allowed access/server rights. • All programs are allowed to perform suspicious behavior. • No program alerts are displayed.

* Component control is disabled by default. If you have turned component control on, it will remain enabled as long as program control is set to High, Medium, or Low. For information about component control, including directions for turning it on, see Enabling Component Control.

To limit the number of alerts you see, you can use the following features:

- Use the **Auto** program control level, which employs the *Auto-Learn* feature.
- Leave SmartDefense Advisor on the Auto setting, to benefit from automatic program settings.

Custom Application Control features

The Custom Application Control Settings window provides several high-security settings that are designed to prevent malicious programs from controlling trusted programs.

1. Select **COMPUTER** | **Application Control | Settings | Advanced Settings** and then click **Application Control.**
2. Specify the settings to apply.

Enable Advanced Application Control	Prevents trusted programs from being used by untrusted programs to circumvent outbound firewall protection.
Enable Application Interaction Control	Alerts you when a process attempts to use another process or when a program launches another program.
Enable Timing Attack Prevention	Detects and stops programs that try to hijack a trusted program's permissions (e.g., to load drivers, change registry keys, or regulate processes). Also known as handle protection. On by default when Application Control is High or Maximum.

Enable Microsoft Catalog Utilization	When enabled, prevents alerts for programs that are cataloged by Windows as known and trustworthy. Enabled by default. (Depending on your settings, ZoneAlarm may still alert you about such programs if they attempt to act as a server outside your Trusted Zone.)
Enable component control	Restricts or monitors individual components, such as DLL files or ActiveX controls, that malware programs may use to access the network. If Application Control is Medium, component control tracks components but does not restrict them. If Application Control is High, it prompts you to allow or deny new components. See Enabling Component Control for details.
Enable services control	Alerts you if untrusted programs attempt to install or modify a service or driver. Active when Application Control is set to High or Maximum. See Understanding services control (on page 107) for more information.

3. Click **OK**.

To learn about the settings on the OSFirewall panel of this dialog, see Configuring OSFirewall protection.

Note - Since some programs that control other programs are legitimate, ZoneAlarm gives the most common ones permission to access the Internet. You can view and adjust individual configurations on the Programs panel.

Configuring OSFirewall protection

OSFirewall protection, which is enabled by default, detects when programs try to use your operating system to perform suspicious and potentially damaging actions on your computer. You can also configure various OSFirewall Special System Protections, which determine whether programs on your computer can perform specific actions such as modifying your Internet Explorer home page or installing ActiveX controls.

See OSFirewall alerts (on page 88) for more details about the kinds of behaviors and alerts that are associated with OSFirewall protection.

To configure OSFirewall settings:

1. Select **Application Control**.
2. In the Application Control area, click **Advanc**ed Settings.
3. In the dialog that appears, select the **OSFirewall** panel.
4. Select or deselect **Enable OSFirewall**, as desired. (To configure any OSFirewall Special System Protections in the next step, you must first enable OSFirewall.)
5. Optionally, configure any OSFirewall Special System Protections. For any action in the list, click the State field and select **Allow**, **Deny**, **Ask**, or **Use Program Setting**. If you choose Use Program Setting, ZoneAlarm security software defers to SmartDefense Advisor settings or to your manual settings.
6. Click **Apply** to save the setting and leave the dialog open, or **OK** to save the setting and close the dialog.

Understanding services control

The services control feature catches dangerous program behaviors that other firewalls have typically ignored. It controls changes to the Windows Services section of your computer's registry file, blocking attempts by untrusted programs to install or modify services or drivers. If such attempts occur, you are alerted and given the choice to allow or deny them.

This protection:

- prevents malware from being installed to start automatically when your computer starts up
- prevents drivers from being loaded into your PC kernel by rootkit malware

You can enable or disable services control in the Application Control Custom Settings, as described in Custom program control features. Services controls activates only when Application Control is set to High or Maximum.

Enabling Component Control

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). ZoneAlarm security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your Application Control and component control settings, ZoneAlarm security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to enable component control. For details about viewing the Components List and modifying component permissions manually, see Managing program components.

By default, component control is turned off, though ZoneAlarm security software does add components to the Components List. If you enable component control and set Application Control to Medium, component control tracks components but does not restrict their activity. If you then reset Application Control to High, component control grants access to all previously known components but prompts you to allow or deny any components discovered subsequently.

For advanced users concerned about component activity, the best practice is to install ZoneAlarm security software on a freshly set up computer, enable component control and set the Application Control level to Medium, and, after ZoneAlarm security software has had a chance to detect all normal components that require access, reset Application Control to High. (For information about the Application Control setting, see Setting the Application Control level ("Setting the program control level" on page 103).)

To enable component control:

1. Select **Application Control**.
2. In the Application Control area, click **Advanc**ed Settings.
   The Custom Application Control Settings dialog appears.
3. On the Application Control panel, select **Enable component control**.
4. Click **OK**.

Setting the SmartDefense Advisor level

Whenever you use a program that requests access, SmartDefense Advisor queries the ZoneAlarm server to determine the policy for that program. You can choose to have SmartDefense Advisor set the permissions for the program automatically, or you can configure program access manually. The SmartDefense Advisor level is set to Auto by default.

If you set SmartDefense Advisor to Auto and there is no advice available for a program, ZoneAlarm security software displays a Program alert prompting you to allow or deny access to the program. ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

For information about setting program permissions manually, see Setting permissions for specific programs (on page 111). You can set SmartDefense Advisor to Manual or Off and set *all* program permissions manually. Or, you can set SmartDefense Advisor to Auto and set manual program permissions *only* when SmartDefense Advisor does not recommend a policy.

To set the SmartDefense Advisor level

1. Select **Application Control.**
2. In the SmartDefense Advisor area, choose your setting.

Auto	In Auto mode, SmartDefense Advisor automatically implements the recommendation returned from the server. Application Control must be set to Medium or High to set SmartDefense Advisor to Auto.
Manual	In Manual mode, you will receive Program alerts when programs request access and can set the permission on your own.
Off	SmartDefense Advisor will not contact the server for program advice.

Viewing logged program events

By default, all Program events are recorded in the Log Viewer.

To view logged program events:

1. Select **Tools** | **Logs**|**Log Viewer**.
2. Select **Program**, from the Alert Type drop-down list.

The following table provides an explanation of the log viewer fields available for Program events.

Field	Explanation
Rating	Event rating based on the **Protection Level** of the security option.
Date/Time	Date and time the event occurred.
Type	Type of program alert that occurred. Possible values for this column include: • Program Access • Repeat Program • New Program
Program	The program (displayed as the application file) that requested access. If a program name is unavailable, refer to the Description field of the Entry Details window.
Source IP	The IP address of the computer sending the request. If the source IP cannot be determined, this field may be left blank.
Destination IP	The IP address of the computer receiving the request. If the destination IP cannot be determined, this field may be left blank.
Direction	Specifies whether the request that caused the event was incoming, outgoing, or occurred as a result of internal traffic on your computer (data).
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /
Count	The number of times this action was taken.
Source DNS	The domain name server of the computer that is sending the request.
Destination DNS	The domain name server of the computer that is receiving the request.

Program event log fields

Viewing logged OSFirewall events

By default, all OSFirewall events are recorded in the Log Viewer.

To view logged OSFirewall events:

1. Select **Tools | Logs| Log Viewer**.
2. Select **OSFirewall**, from the Alert Type drop-down list.

The following table provides an explanation of the log viewer fields available for OSFirewall events.

Field	Explanation
Rating	Event rating based on the **Protection Level** of the security option.
Date/Time	Date and time the event occurred.
Type	Type of OSFirewall alert that occurred. Possible values for this column include: • Process • Message • Module • Registry • File • Execution • Driver • Physical memory
Subtype	The specific event that initiated the Type of access requested (for example, OpenThread would be a subtype of Process).
Data	The path to the file that was attempting to be modified.
Program	Displays the path to the program that performed the behavior.
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /manual or /auto to indicate whether the action was performed by you or by SmartDefense Advisor.
Count	The number of times this action was taken.

OSFirewall event log fields

Setting permissions for specific programs

In some cases, you may want to specify different settings for an individual program than the global Application Control level will allow. For example, if you wanted to allow access to a particular program, but keep security High for all other programs, you could set the permission for that program to **Allow**.

Note - After you manually set permissions for a program, the permissions for that program will not change even if you later set the SmartDefense Advisor level to Auto. To benefit from automatic program advice, remove the program from the Programs List, then set the SmartDefense Advisor level to Auto.

•

Using the programs list

The programs list provides an overview of the programs on your computer that have tried to access the Internet or the local network. For each program, the list provides detailed information about its current state, trustworthiness, and the functions it is allowed to perform.

You can sort the programs in the list by any column by clicking on column header. As you use your computer, ZoneAlarm security software detects every program that requests network access and adds it to the programs list.

To access the Programs List, select **Application Control**| **View Programs**.

Selecting a program name in the list displays program information in the Detail area below the list.

The **SmartDefense** and **Trust Level** columns indicate OSFirewall Protection for your computer and specify whether a program is allowed to perform operating system-level actions like changing TCP/IP parameters, loading or installing drivers, or changing your browser's default settings.

Active

Indicates the current status of a program. A green circle indicates that the program is currently running.

Programs

The name of the program.

SmartDefense Advisor

The SmartDefense Advisor column indicates where the program policy comes from. The column may contain any of the following designations:

- **Auto**—SmartDefense Advisor determines the program policy, unless a recommendation is not available. (Note that, if SmartDefense Advisor is turned on, the SmartDefense Advisor column will still say Auto, since the permissions will change to conform to any SmartDefense Advisor recommendations that come out later.)
- **Custom**—You determined the program policy manually. If you change a program's permissions (by changing a value in any of the columns in the program's row, for example), the SmartDefense Advisor column displays "Custom" for that program.
- **System**—SmartDefense Advisor determines the program policy, and the program is used by your operating system.

Important - Manually changing the policy for "System" programs could interfere with the normal functions of your computer.

Trust Level

The Trust Level determines the actions that a program is allowed to perform. The Trust Levels are Super, Trusted, Restricted, Ask, Kill, and No Enforcement.

A program's Trust Level setting is determined by its policy. ZoneAlarm security software assigns policies to known programs automatically. The SmartDefense Advisor security team constantly monitors programs for changes in behavior and trustworthiness and updates the programs permissions accordingly. A program with a Trust Level setting of Super today, might have a Trust Level of Restricted tomorrow, if security experts determine that the program could pose a risk to your computer. If you change a program's policy setting from Auto to Custom, however, it will no longer be monitored for changes in Trust Level. For this reason, it is recommended that you keep the default settings for your programs. Refer to the table below for a description the symbols used in this list.

Outbound and Inbound

The Outbound and Inbound columns refer to a program's right to send and retrieve information from the Internet or networks in the Trusted Zone.

Server

The Check Point Document Security Client can connect to the Check Point Document Security Policy Server, as a stand-alone server or integrated with Microsoft RMS server. Alternatively, you can deploy the client with a Microsoft RMS Server on Windows 2003 or 2008.

Basic server actions:

- Gives keys to authorized users.
- Lets you create and manage policies.
- Collects system audit data.

Send Mail

Allows a program to send and receive e-mail.

Refer to the table below for a description of the symbols used in this list.

Symbol	Meaning
	The program is currently active.
	The program is allowed access/server rights.
	When this symbol appears in the Access or Server columns, it means that ZoneAlarm security software will display a Program alert when the program asks for access, server rights. When this symbol appears in the Trust Level column, it means that ZoneAlarm security software will display a Suspicious Behavior alert when a program performs actions considered suspicious.
	The program is denied access/server rights.
	Super access. Program can perform suspicious actions without seeking permission. No alerts will be displayed.

Symbol	Meaning
	Trusted access. Trusted Programs can perform suspicious actions without seeking permission, but unknown programs must ask for permission.
	Restricted access. Program can perform trusted-level actions but cannot perform suspicious actions.
	No access. Programs marked with the No access (Kill) symbol cannot run.
	No enforcement. Program is not monitored at all and can perform any action whatsoever. This setting can pose a security risk.

Program List symbols

For more information about what program actions are considered suspicious, see OSFirewall alerts (on page 88).

Adding a program to the programs list

If you want to specify access or server permission for a program that does not appear on the programs list, you can add the program to the list and then grant the appropriate permissions.

To add a program to the programs list:

1. Select **Application Control**| **View Programs**, then click **Add**.
2. In the dialog that appears, locate the program you want to add, then click **Open**.

   Be sure to select the program's executable file (for example, program.exe).

To edit a program on the programs list:

1. Select **Application Control**| **View Programs**.
2. Select a program in the Programs column and choose one of the available options.

Options	Opens the Program Options dialog box, in which you **can customize security options and create expert rules for programs ("Setting**

	program options for a specific program" on page 116).
Properties	Opens your operating system’s properties dialog box for the program.
Remove	Deletes the program from the list.

Granting a program permission to access the Internet

Many of your most commonly used programs can be automatically configured for safe Internet access. To determine whether a program was configured manually or automatically, select the program in the Programs List and refer to the Policy field in the Entry Details area.

To grant a program permission to access the Internet:

1. Select **Application Control**| **View Programs**.
2. In the Programs column, click the program for which you want to grant access, then select **Allow** from the shortcut menu.

For information about granting programs permission by responding to an alert, see New Program alert (on page 63).

Note - Built-in rules ensure a consistent security policy for each program. Programs with access to the Public Zone also have access to the Trusted Zone, and programs with server permission in a Zone also have access permission for that Zone. This is why (for example) selecting Allow under Trusted Zone/Server automatically sets all of the program’s other permissions to Allow.

Granting a program permission to act as a server

Exercise caution when granting permission for programs to act as a server, as Trojan horses and other types of malware often need server rights in order to do mischief. Permission to act as a server should be reserved for programs you know and trust, and that need server permission to operate properly.

To grant a program permission to act as a server:

1. Select **Application Control**| **View Programs**.
2. In the Programs column, click the program for which you want to grant server access, then select **Allow** from the shortcut menu.

Granting send mail permission to a program

To enable your e-mail program to send e-mail messages and to enable protection against e-mail threats, grant send mail permission to your e-mail program. For more information about protecting your e-mail, see E-mail protection (on page 138).

To grant send mail permission to a program:

1. Select **Application Control**| **View Programs**.
2. Select a program from the list, then click in the **Send Mail** column.
3. Select **Allow** from the shortcut menu.

Note - You also can access the Program Options dialog by selecting a program name and clicking **Options**.

Setting program options for a specific program

How a program is authenticated, whether it uses Outbound MailSafe protection, or is held to privacy standards, is determined globally by setting the Program Control level. You can modify these and other settings on a per-program basis from the Programs List.

- Setting Advanced Program Control options
- Disabling Outbound Mail protection for a program
- Setting Filter options for a program
- Setting authentication options
- Setting passlock permission for a program (on page 118)

Setting Advanced Application Control options

Advanced Application Control tightens your security by preventing unknown programs from using trusted programs to access the Internet, or preventing hackers from using the Windows CreateProcess and OpenProcess functions to manipulate your computer.

To enable Advanced Application Control for a program:

1. Select **Application Control**| **View Programs**.
2. In the Programs column, select a program, then click **Options**.
   The Program Options dialog appears.
3. On the **Security panel**, choose your Advanced Application Control options.

This program may use other programs to access the Internet	Allows the selected program to use other programs to access the Internet.
Allow Application Interaction	Allows the selected program to use OpenProcess and CreateProcess functions on your computer.

4. Click **OK**.

Disabling Outbound Mail protection for a program

By default, Outbound Mail protection is enabled for all programs. Because the ability to send e-mail is not a characteristic of all programs, you may choose to disable Outbound Mail protection for any program that does not require it.

To disable Outbound Mail protection for a program:

1. Select **Application Control**| **View Programs**.
2. Select a program from the list, then click **Options**.
   The Program Options dialog appears.
3. Select the **Security** panel.
4. Clear the check box labeled **Enable Outbound MailSafe Protection for this program**.

Note - This check box will not appear unless the SendMail permission for this program is set to Allow.

5. Click **Apply** to save your changes, then click **OK**.

For more information about Outbound MailSafe Protection, see Outbound MailSafe protection (on page 138).

Setting authentication options

You can specify whether a program is authenticated by using its full pathname or by its components. By default, all programs are authenticated by their components.

To specify an authentication method:

1. Select **Application Control**| **View Programs**.
2. Select a program from the list, then click **Options**.
   The Program Options dialog appears.
3. Select the **Security** panel.
4. Under Authentication, select the check box beside the option you want, then click **OK**.

Authenticate components	Highest security setting--authenticates each component of a program.
Authenticate program by full pathname only	Lower security--ZoneAlarm security software will use only file path information to authenticate the program.
Program changes frequently	Lower security--if this option is selected, ZoneAlarm security software will use only file path information to authenticate the program and the MD5 signature will not be checked.

5.

Setting passlock permission for a program

When the Internet Lock is engaged, programs given passlock permission can continue to access the Internet. If you grant passlock permission to a program, and that program uses other applications to perform its functions (for example, services.exe), be sure to give those other programs passlock permission as well.

To grant or revoke passlock permission:

1. Select **Application Control**| **View Programs**.
2. Select a program from the list, then click **Options**.
3. Select the **Enable Pass Lock** check box.
4. Click **Apply**, then click **OK**.

Managing program components

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). ZoneAlarm security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your Application Control and component control settings, ZoneAlarm security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to access the Components List and how to change component permissions. For details about enabling component control, see Enabling Component Control.

The Components List contains a list of program components for allowed programs that have tried to access the Internet or the local network. The Outbound column indicates whether the component is always allowed access, or whether ZoneAlarm security software should alert you when that component requests access. By default, the Components List is organized in

alphabetical order, but you can sort the components in the list by any column by clicking on the Component column header.

To access the Components List:

Select **Application Control**| **View Components**.

To grant access permission to a program component:

1. Select **Application Control|View Components**.
2. Select a component from the list, then click in the Outbound column.
3. Select **Allow** from the shortcut menu.

Creating expert rules for programs

By default, programs given access permission or server permission can use any port or protocol, and contact any IP address or host at any time. Conversely, programs that you block have no access rights at all. By creating expert rules for particular programs, you can heighten protection against hijacked programs by specifying ports and protocols, source and destination addresses, and time and day ranges during which activity is either allowed or denied. You can also apply tracking options to specific types of traffic in order to see alerts or generate log entries when allowed program traffic occurs, enable or disable rules at will, and apply multiple, ranked rules to a program.

Note - If you created port rules for Programs in a version of ZoneAlarm security software, prior to 4.0, those port rules will be automatically converted to expert rules and visible in the Expert panel of the Program Options dialog. To access the Expert panel, select **Application Control**| **View Programs**, then click **Options**.

Creating an expert rule for a Program

Expert rules for programs are enforced in the order they are ranked. Therefore, when you create expert rules for a program, make sure that the last rule you create for that program is a "Block All" rule.

To create an expert rule for a program:

1. Select **Application Control** | **View Programs**, then click **Options**.
2. Select **Expert Rules**, then click **Add**.

   The Add rule dialog appears.
3. Create Expert Program rule.

Note - The Add rule dialog contains the same fields and options that are available when you create Expert Firewall rules. Note, however, that IGMP and Custom protocols cannot be applied to expert rules for Programs. See Creating expert firewall rules (on page 36).

4. Click **OK**.

Removing expert rules

Expert firewall rules (created in the Firewall | Expert panel) cannot be directly applied to a single program. If the rule is enabled, it is applied globally. Similarly, an expert rule you created for one program cannot be directly applied to another program.

To remove an Expert rule:

1. Select **COMPUTER| Application Control** | **View Programs**.
2. Select the program for which you want to remove an Expert rule, and then click **Options**.
3. Click **Expert Rules**, select the rule you want to eliminate, and then click **Remove**.
4. Click **Apply**, then click **OK**.

Browser security

ZoneAlarm security software adds a toolbar to your browser that protects your computer and your personal data and privacy while you are on the web.

Using browser security

You know that ZoneAlarm browser security is on you when you see the ZoneAlarm toolbar in your browser.

The ZoneAlarm browser security toolbar adds the following important protections.

- Warns you when you go to sites that do not have adequate security credentials.
- Detects known and unknown phishing Web sites.
- When *virtualization* is enabled, it can stop malicious zero day drive-by downloads, meaning malware that is not yet known by anti-virus and anti-spyware engines and has no known solution. (Not included in some versions.)
- Lets you choose a Privacy Browser option when you want to leave no trace on your computer of what you've typed or where you've been. (Not included in some versions.)

- Checks anything you download from the Web for malware, using a sophisticated multi-layer scanning process. (Not included in some versions.)
- Blocks the processes that keylogger and screen grabber malware use to secretly record your keystrokes or onscreen activity. This helps ensure that even keyloggers or screen grabbers that have not yet been discovered are rendered harmless. (Not included in some versions.)

See the Help Center provided in the ZoneAlarm browser security toolbar for full details.

Accessing ZoneAlarm browser security Help and troubleshooting:

Open the online Browser Security Help Center from your browser toolbar:

1. With ZoneAlarm browser security enabled, open a Web browser.
2. From the **ZoneAlarm browser toolbar menu**, choose **Help**.

Turning browser security on and off:

ZoneAlarm browser security performs much of its work behind the scenes, until it needs to warn you about a danger or let you know the results of a download scan.

To turn browser security or off from ZoneAlarm:

1. Select **Browser Security.**
2. Click **On** or **Off**.

To turn browser security on or off from your browser:

1. In your browser window, choose **View | Toolbars**, and then select or deselect "Browser security toolbar."
2. Restart your browser.

The integrated antivirus and anti-spyware feature protects your computer against viruses and spyware in a single powerful operation. Multiple scanning options automatically detect viruses and spyware and render them harmless before they can damage your computer.

Spyware and virus Protection

The anti-virus/anti-spyware engine keeps known and unknown malware from affecting your computer by scanning files and comparing them to a database of known malware and against a set of characteristics and patterns (heuristics) that reflect malware behavior. Files can be scanned as they are opened, closed, executed, or as part of a full computer-wide scan. If a virus is detected, ZoneAlarm security software renders it harmless, either by repairing or denying access to the infected file.

- Turning on virus and spyware protection
- Scheduling regular scans

- Keeping virus definitions up-to-date (on page 122)

Turning on virus and spyware protection

If you chose not to turn on the anti-virus protection feature in the Configuration Wizard following installation, you can turn it on manually.

Important - The ZoneAlarm Anti-virus protection feature is incompatible with other virus protection software. Before you turn on the Anti-virus protection feature, you must uninstall any other anti-virus software from your computer, including suite products that include virus protection among their features.

To enable virus and spyware protection:

1. Select **COMPUTER | Anti-virus & Anti-Spyware**.
2. On **Anti-virus/spyware** panel, select **On**.

Scheduling regular anti-virus scans

ZoneAlarm is set to run regular anti-virus scans, at varying levels of depth, periodically. You can customize the depth, time, and frequency of these scans.

Note: If your computer is not on when the scheduled scan is set to occur, the scan will occur fifteen minutes after your computer is restarted.

To customize the scan schedule:

1. From the **Tools** menu, choose **Scheduled Scans**.
2. In the window that appears, specify scan frequencies and times for each type of scan (described below) that you want to run, then click Apply.

- **Quick Scan:** Fastest. Scans only Windows folders, Startup folders, and folders linked to startup items, which are common places for hackers to place viruses. (Programs in these folders can run automatically without permission, which creates the most risk.)
- **Normal Scan:** Fast, default scan. By skipping archive and non-executable files you get a quicker scan with minimal risk of missing viruses that could self-activate.
- **Deep Scan:** Very thorough. Recommended every six months or after exposure to a virus outbreak. Scans all files and folders, and scans for rootkits. Skips archive files which pose minimal risk because they cannot self-activate

Keeping virus definitions up-to-date

Your virus signature definition files are automatically updated regularly.

What are virus signature definitions?

Every virus or spyware application contains unique identification information, known as its signature definition file. Security software uses these files to detect viruses and spyware on your computer.

As new viruses or spyware applications are discovered, your security software updates its databases with the signature files it needs to detect these new threats.

Therefore, your computer is vulnerable to viruses and spyware whenever its database of virus signature definitions files becomes outdated. But, don't worry, because:

- By default, your virus definition files are automatically updated regularly.
- If you hear of an outbreak and want to get the latest updates immediately, select **Update** in the main window.

To customize automatic signature updates:

1. From the **Tools** menu, select **Schedule Tasks.**
2. Next to **Anti-virus Update** choose an option from the Frequency menu.
3. Click **Apply**.

Customizing virus protection options

In addition to choosing the type of scan you want to perform, you also can specify the method used to detect viruses, and set treatment methods.

ZoneAlarm security software provides several types of virus scans to keep your computer and data safe: system scans, on-access scans, and e-mail scans.

- Specifying scan targets (on page 123)
- Choosing a scan mode (on page 125)
- Configuring on-access scanning
- Enabling automatic virus treatment
- Specifying scan options (on page 126)
- Excluding items from virus scans

Specifying scan targets

You can specify which drives, folders, and files are scanned when a scheduled or manual system scan occurs. Exclude or include an item in the scan by selecting the checkbox beside it. By default, ZoneAlarm security software only scans local hard drives.

The table below provides an explanation of the icons shown in the Scan Targets dialog box.

Icon	Explanation
	The selected disk and all sub-folders and files will be included in the scan.
	The selected disk and all sub-folders and files will be excluded from the scan.
	The selected disk will be included in the scan, but one or more sub-folders or files will be excluded from the scan.
	The selected folder will be excluded from the scan, but one or more sub-folders or files will be included in the scan.
	The selected folder will be included in the scan. A gray check mark indicates that scanning of the folder or file is enabled because scanning has been enabled for a higher level disk or folder.
	The selected folder will be excluded from the scan. A gray "x" mark indicates that scanning of the folder or file is disabled because scanning has been disabled for a higher level disk or folder.

Icons indicating scan targets

Note - Keep in mind that your Scan Mode settings override your Scan Target settings. For example, regardless of the folders you select as your Scan Targets, if Quick Scan is your Scan Mode then the only folders scanned are Windows and Startup folders. See also Choosing a scan mode (on page 125).

To specify scan targets:

1. Select **COMPUTER | Anti-virus & Anti-Spyware** and click **Settings**, then click **Advanced Settings**.
2. Under Virus Management, select **Scan Targets**.
3. Select the drives, folders, and files to be scanned.

   The **Other** option listed refers to RAM disks and any unknown drive *other than* floppy, removable, local, remote, CD, and network drives.
4. Select or clear the **scan boot sectors for all local drives** check box.
5. Select or clear the **scan system memory** check box, then click **OK**.

Choosing a scan mode

Virus **scan modes** apply to the scans that run according to a regular schedule or when you click a Scan button.

Choosing a Scan Mode for scheduled scans:

See Scheduling regular anti-virus scans.

Choosing a Scan Mode for on-demand scans:

1. Select **COMPUTER** | **Anti-virus/spyware** | **Settings** | **Advanced Options**.
2. Choose a **Scan Mode:**

Quick Scan	**Fastest**. Scans only Windows folders, Startup folders, and folders linked to startup items, which are common places for hackers to place viruses. (Programs in these folders can run automatically without permission, which creates the most risk.)
Normal Scan	**Fast, default scan**. By skipping archive and non-executable files you get a quicker scan with minimal risk of missing viruses that could self-activate.
Deep Scan	**Very thorough**. Recommended every six months or after exposure to a virus outbreak. Scans all files and folders, and scans for rootkits. Skips archive files which pose minimal risk because they cannot self-activate.

Note - Your Scan Mode settings override your Scan Target settings. For example, regardless of the folders you select as your Scan Targets, if Quick Scan is your scan mode, then the only folders scanned are Windows and startup folders.

Configuring on-access scanning

On-access scanning protects your computer from viruses by detecting and treating viruses that may be dormant on your computer. It is on by default and supplies the most active form of malware protection, so we recommend you keep it enabled.

Files are scanned for viruses as they are opened, executed, or saved, thereby allowing immediate detection and treatment of viruses.

Note - Archive files, such as .zip files, are scanned by on-access scanning when you open them.

To enable on-access scanning:

1. Select **COMPUTER | Anti-virus & Anti-Spyware,** click **Settings**, then click **Advanced Settings.**
2. Select **On-Access Scanning**.
3. Select **Enable On-Access Scanning**, and optionally specify a mode, then click **OK**:

Scan when reading and writing	(Recommended) Scans a file when it's opened, saved, or executed.
Scan in Smart Mode	Scans files when they are opened, saved, or executed, and expedites this process by leveraging information from previous scans.
Scan when reading	Scans a file when it's opened or executed.

Enabling on-access scanning of network files

You can enable on-access virus/spyware scanning of the files that exist on any drives or computers you are connected to on a network. Note that this option may not be necessary, and may slow performance, if these drives already have full security protection.

1. Select **COMPUTER| Antivirus & Anti-spyware**, click **Settings**, and then click **Advanced Settings.**
2. Select **On-Access Scanning**.
3. Select **Enable scanning of network files**.

Specifying scan options

These options apply to on-demand scans and on-access scans. These options do not apply to contextual (i.e., select item and right-click) scans.

To specify virus scan options:

1. Select **COMPUTER | Anti-virus & Anti-Spyware**, then click **Settings, then click Advanced Settings.**
2. Under **Virus Management**, select **Scan Options**.
3. Select your desired settings, then click **OK**.

Skip if the object is greater than	This option improves scan time without increasing risk, as virus files are usually smaller than 8 MB. While large files ignored by the scan may contain viruses, these viruses can still be caught by on-access scanning, assuming you have on-access enabled. Enter a maximum object size in the **MB** field.
Enable riskware***** scanning	Warns you about programs that could potentially be a security risk if accessed or controlled by hackers. Riskware includes common programs, such as chat and web downloader programs, that are known to have security vulnerabilities. They be used to cause damage or steal information. When riskware is detected, ZoneAlarm asks your permission to let it run.*****
Enable cpChecker	Optimizes performance by minimizing scanning according to rules that leverage prior scan data. Works on limited file sizes and formats. Most efficient when cpSwift is also enabled.
Enable cpSwift	Optimizes performance by minimizing scanning according to rules that leverage prior scan data. Works on any file formats, sizes, and types. Most efficient when cpChecker is also enabled.
Enable ADS scanning	Scans alternative data streams (ADS), which can sometimes hide malware in otherwise benign files.
Enable heuristics scanning	Scans files for specific information or characteristics associated with malware. Adds another layer of security by detecting viruses or spyware not yet known to virus signature databases.
Enable mailbox scanning	Scans mailbox files (such as the.pst and .ost data files from Microsoft Outlook) during system-wide anti-virus scans.
Assume Microsoft files are safe	Prevents false positive results by assuming files signed by Microsoft are safe.

Enable automatic treatment	Automatically attempts to treat files that contain viruses. If a file cannot be treated, it's placed in Quarantine so that it cannot harm your computer. **Note:** Web and Email scanning always operate in automatic treatment mode. You cannot disable automatic treatment for Web and Email scanning.

***Other programs that may be detected as riskware include:** remote administration programs, FTP servers, proxy servers, password recovery tools, monitoring programs, automatic dialing programs, telnet servers, Web servers, computer tools, network tools, peer-to-peer client programs, SMTP clients, Web toolbars, and known fraudulent programs. Of these types of programs, only those known for security vulnerabilities will be detected as riskware.

Excluding items from virus scans

Excluding items from virus scans can be useful in the following circumstances:

- When you don't want ZoneAlarm to scan certain directories, files, or programs that you know to be safe, see Excluding files from virus scans.
- If a scan reports as a virus a program you know to be safe, see Excluding detected viruses from scans.

Excluding files from virus scans

You may want to exclude certain files and programs you know to be safe.

To specify items that should be ignored by virus scans:

1. Select **COMPUTER** | **Antivirus & Anti-spyware**, then click **Settings.**
2. Click **Exceptions**.
3. Click the **Add File** button and choose from the **Select type** menu:

On-Access scan	Excludes the selected file(s) from on-access scans, which occur when a file is opened, executed, or saved.
Trusted Process	Choose this if you want to exclude an executable (.exe) file from scans.

4. Do one of the following:
   - Click **Browse** to select a file you want to exclude.
   - To exclude a drive or group of files, enter them into the **Select exception** field using one of the formats shown in the Browse dialog box.
5. Click **OK**.

Excluding detected viruses from scans

Some benign applications may be mistaken as viruses during a system or on-access scan. If an application shows up in the Scan Results but you are certain it is safe, you can exclude it from anti-virus scans by adding it to the exceptions list.

To exclude a suspected virus from future scans:

- When a virus **Scan Results** dialog appears, right-click programs that you want to exclude and choose **Ignore Always**.

The program is added to exceptions list and will no longer be detected during virus scans.

Customizing behavioral scanning

Behavioral scanning detects new malware that is not yet tracked by anti-virus databases. For example, it can detect a process attempting to install a driver to gain access to your operating system. It can also detect rootkit-like behaviors that would set up access for hackers.

Behavioral scan detection does two different things:

- If the detected behavior is clearly dangerous, it moves the program to Quarantine so it poses no threat to your computer.
- If the detected behavior is suspicious, you are prompted to make a choice of allowing the activity or not.

Customizing behavioral scanning:

Open the **Anti-virus / Anti-spyware | Settings | Behavioral Scan** panel to view all the behaviors that ZoneAlarm considers suspicious or dangerous. Deselect any behaviors that you don’t want monitored.

Note: The dangerous behaviors list on this panel is dynamically updated as your product receives updates.

Performing a scan

There are several ways you can run anti-virus/spyware scans on your computer. Once a scan starts, a dialog appears from which you can pause or cancel the scan if you want to.

Scan	How to run it
On-demand (manual) system scan	Click **Scan i**n the upper right corner.
Scheduled system scan	System scans are set to run regularly by default. You can set how often they run. See Scheduling regular

Scan	How to run it
	scans.
Contextual scan (manual file scan	To instantly scan a specific file, right-click the file, then choose **Scan with ZoneAlarm Anti-virus**.
On-access scan	Open a file—the file is instantly scanned in the background upon opening. On-access scanning is enabled by default. See Configuring on-access scanning. ("Configuring on-access scanning" on page 125)

How to perform different types of scans

You may run up to five scans simultaneously. Scans are performed in the order in which they are initiated. System scans provide another level of protection by allowing you to scan the entire contents of your computer at one time. System scans detect viruses that may be dormant on your computer's hard drive, and if run frequently, can ensure that your anti-virus signature files are up to date.

Because of the thorough nature of full-system scans, some can take a while to perform. To avoid any impact on your workflow, you can schedule system scans to run at a time when you are least likely to be using your computer. See Scheduling regular anti-virus scans.

During scans, ZoneAlarm security software displays a special notification icon nd provides a notification icon menu option for viewing scan status.

- Right-click the notification icon icon and choose **View Scan** to check on scan status.
- Clicking **Pause** in the Scan dialog while a scan is being performed will stop the current scan only. On-access scanning will not be disabled. Click **Pause** again to resume the current scan.

Rootkit scanning

ZoneAlarm software works to block rootkits from getting onto your computer, but does not automatically scan for them. Rootkits are detected and treated in Deep Scan mode.

To perform rootkit scanning and removal:

1. Set **Anti-virus/Anti-spyware | Advanced Options | Scan Modes** option to **Deep Scan**.
2. Click **Scan.**

Understanding virus scan results

If anything unusual is detected in a scan, you'll see it in a Scan Results dialog that appears.

- The items listed under **Auto Treatment** have already been treated--you do not need to take further action.

- The **Active Items** area of the dialog lists any infections that could not be treated automatically. To accept the suggested treatments in the Treatment column, click **Apply**.

Tip: If the scan results list a program that you are certain is safe, you can exclude it from future scans. See Excluding detected viruses from scans.

Name

Give the rule a descriptive name. The name can include spaces.

Double-click in the **Name** column of the rule to add or change a name.

Treatment

Specifies the treatment applied to the infection. Possible values are Quarantined or Deleted.

Security Risk

Indicates the risk level of the infection. All viruses are considered High risk.

Path

The location of the virus on your computer.

To view spyware in quarantine:

1. Select **Anti-virus / Anti-spyware** | **Quarantine.**
2. Choose **Spyware** from the Quarantined View drop-down list.
3. Optionally, select a spyware entry in the list and click **Delete** (to delete it from your computer), **Restore** (to restore it to your computer), or **More Info** (to consult SmartDefense Advisor for more information about it).

The spyware view in quarantine contains the following columns of information:

Type

Specifies whether the site is a Security Alliance partner or a Custom site.

Status

Tells you whether the file has been repaired, deleted, or remains infected. If ZoneAlarm security software was unable to treat the item, a **What to do next** link may appear here. This link will direct you to further information and instructions.

Information

Provides more detail about the infection. To get more information about a virus or spyware, click the **Learn more** link.

Detail

Lists the location of virus traces. Advanced users may find this information useful for tracking down viruses that cannot be treated automatically.

Treating virus files manually

If you do not have automatic treatment enabled, or if a file could not be repaired automatically, you can attempt to treat it manually from the Scan Results dialog.

To treat a file manually:

1. In the Scan Results dialog, select the item you want to treat.
2. Click the button for the treatment option you want:

Treat	Tries to repair the selected file.
Ignore once	Ignores this file this one time. This is a good choice if you suspect the file is safe and you want to see if it's detected in the next scan, after your antivirus signatures have been updated.
Ignore always	If you are sure the file is safe and don't want to receive anymore detection alerts about it, choosing "Ignore always" tells the antivirus not to scan this file anymore.

3. When you have finished treating files, click **Close**.

Note - If the results of a virus scan contain Error, No treatment available, or Treatment failed, it means that there is not yet a way to automatically remove the virus without risking the integrity of your computer or other files. In some cases, there may be manual treatments available to you. To find out, enter the name of the virus along with the word "removal" into a search engine, such as Google or Yahoo, to locate removal instructions. Otherwise, know that we're constantly

researching viruses and developing safe ways to remove them.

Repairing files in an archive

If the infected file is located in an archive file (such as a .zip file), ZoneAlarm security software will not be able to treat it (either by repairing, deleting, or placing it in Quarantine) while the file is still included in the archive.

To repair a file in an archive:

1. Select **COMPUTER | Anti-virus & Anti-Spyware**, click **Settings**, then click **Advanced Settings**.
2. Select **On-Access Scanning**, then select the **Enable On-Access Scanning** check box.
3. Click **Apply**, then click **OK**.
4. Open the file that was specified in the Scan Results dialog from within an archival utility, such as WinZip.

   On-access scanning will scan the file for infections. The Scan Results dialog will appear with the results of the scan. If the file still cannot be repaired, see Treating virus files manually (on page 132).

Viewing logged virus events

By default, all Virus events are recorded in the Log Viewer.

To view logged Virus events:

1. Select **Tools | Logs|Log Viewer**.
2. Select **Virus**, from the Alert Type drop-down list.

The table below provides an explanation of the log viewer fields available for Virus events.

Field	Information
Date	The date of the infection.
Type	The type of event that occurred. Possible values for this field include: • Update • Scan • Treatment • E-mail
Virus name	The common name of the virus. For example, *iloveyou.exe*.

Field	Information
Filename	The name of the infected file, the name of files being scanned, or the name and version number of update and/or engine.
Action Taken	How the traffic was handled by ZoneAlarm security software. Possible values include: • Updated, Update cancelled, Update Failed • Scanned, Scan cancelled, Scan Failed • File Repaired, File Repair Failed • Quarantined, Quarantine Failed • Deleted, Delete Failed • Restored, Restore Failed • Renamed, Rename Failed
Actor	Whether the action was manual or auto.
E-mail	If the virus was detected in e-mail, the e-mail address of sender of the infected message.

Virus event log fields

Viewing virus and spyware protection status

The **Anti-virus/spyware** panel displays the status of your virus and spyware protection. From this area you can:

- Verify that virus and spyware protection is turned on.
- The dates and times of your last scan(s).
- Update definition files.
- Invoke a scan.
- View results of latest scan.
- Access advanced settings.

The section that follows describes the status information located on the main panel of the Anti-virus / spyware panel.

- Monitoring virus protection (on page 135)
- Enabling and disabling Anti-virus Monitoring (on page 136)
- Viewing Status Messages in the Anti-virus Monitoring panel (on page 136)

- Performing a scan

Monitoring virus protection

One of the most important things you can do to protect your computer against viruses is to install an anti-virus software product. Once installed, however, the anti-virus software must be kept up to date to ensure protection against new viruses as they are created.

No matter which anti-virus software product you use, if you find yourself in either of the following situations, you are putting your computer at risk for virus attack:

- Your trial or subscription period has expired.
- Your virus signature files are out of date.

Anti-virus Monitoring is a secondary defense system that tracks anti-virus software you have installed on your computer and lets you know when that anti-virus software is out-of-date or turned off. This secondary alerting system works as a back-up to your anti-virus software's built-in warning and update system. Most anti-virus products include automatic updating, and alert you when your virus definition files become outdated. Note that not all anti-virus products are supported by this feature.

- Monitoring Coverage (on page 135)
- Monitoring product status (on page 136)

- Monitoring antivirus status alerts

- Enabling and disabling Anti-virus Monitoring (on page 136)
- Viewing Status Messages in the Anti-virus Monitoring panel (on page 136)

Monitoring Coverage

Anti-virus Monitoring currently detects anti-virus software from these popular manufacturers:

- Symantec
- McAfee
- Computer Associates
- Trend Micro

If you use a different anti-virus product, Anti-virus Monitoring will not recognize it at this time. This does not mean that your ZoneAlarm product is malfunctioning; your security remains as strong as ever. ZoneAlarm security software will be adding the ability to recognize more products over time. If your anti-virus product is not currently supported, you may simply turn off the Anti-virus Monitoring feature. Do not worry-- Anti-virus Monitoring is monitoring only and has no affect on the firewall and no direct affect on security.

Monitoring product status

In these products, you will see an Anti-virus Monitoring panel. From this panel you can view the status of your anti-virus product. You can also turn monitoring on or off, or you can turn on or off just the monitoring alerts.

To turn off Monitoring and Monitoring alerts:

1. Select **Anti-virus Monitoring**.
2. In the **Monitoring** area, select **Off**.
3. Clear the check box **Notify me of anti-virus security lapses**.

Monitoring antivirus status alerts

In products where there is no Anti-virus Monitoring panel because the products are equipped with ZoneAlarm Anti-virus, there are monitoring alerts. When ZoneAlarm Anti-virus is turned off, the Anti-virus Monitoring feature is activated. Monitoring can be turned off from any monitoring alert, or from the Advanced Options dialog.

To turn off Monitoring

1. Select **Tools** | **Logs | Main**.
2. Select the **Alerts Events** panel.
3. Clear the following check boxes:
   - Anti-virus protection not found
   - Anti-virus events
4. Click **OK**.

Enabling and disabling Anti-virus Monitoring

If you do not have ZoneAlarm Anti-virus installed and are using another anti-virus software product, Anti-virus Monitoring will be enabled by default. In addition, you can choose to enable Monitoring alerts, which will appear whenever a lapse in protection is detected.

To enable or disable Anti-virus Monitoring:

1. Select **Anti-virus Monitoring**.
2. In the Anti-virus Monitoring area, select **On**.

Viewing Status Messages in the Anti-virus Monitoring panel

The Status area of the Anti-virus Monitoring panel displays the current state of your installed Anti-virus products, as well as the state of Anti-virus Monitoring.

Viewing items in quarantine

In some cases, items detected during a virus or spyware scan cannot be treated or removed automatically. These items are usually placed into Quarantine so that they are rendered harmless but preserved so that they may be treated in the future after an update to your virus and spyware signature files.

Any files in Quarantine are completely neutralized and isolated -- your computer is safe from them.

To see viruses in Quarantine:

- Select **COMPUTER** | **Anti-virus / Anti-spyware | Settings | Quarantine**.

The Quarantine panel includes these options:

Delete	Deletes selected file.
Restore	Restores selected file to original folder on your computer.
More Info	Shows more information about selected file.
Rescan when new signatures are received, auto roll back if scans are negative	When enabled, if a quarantined object is found safe by new virus signature scans, it's restored to the folder it was in before it was quarantined.

When does ZoneAlarm automatically quarantine a file?

- When heuristic scanning finds that the file resembles a known threat or has a malware-like structure.
- When behavioral scanning detects that operations attempted by the file are suspicious and dangerous.

Parental Controls help you protect your kids from risky and inappropriate content online.

You can limit time spent online, block pornography, hate sites, questionable chat rooms, online gambling, profanity and more.

If parental controls are included in your product, here's how to install them:

1. Click **Internet | Parental Controls.**
2. Next to Parental Controls, click **Install**, and follow the onscreen instructions to complete the installation.

Once it's installed, to open Parental Controls:

1. Click **Internet | Parental Controls.**
2. Next to **Parental Controls**, click **Settings.**

   The full Parental Controls window appears.

For details on configuring and using your Parental Control features, select **Help** in the upper left corner of the Parental Controls window.

E-mail protection

Worms, viruses, and other threats often use e-mail to spread from computer to computer. MailSafe protects your friends, co-workers, and others in your address book and helps keep destructive viruses from spreading. The Junk E-mail filter blocks out spam.

Understanding e-mail protection

Attaching files to e-mail messages is a convenient way of exchanging information. However, it also provides hackers with an easy way of spreading viruses, worms, Trojan horse programs, and other malware.

The outbound MailSafe feature stops worms from mass-mailing themselves to everyone you know.

- Outbound MailSafe protection (on page 138)
- Enabling Outbound MailSafe protection (on page 138)

Outbound MailSafe protection

Outbound MailSafe protection alerts you if your e-mail program tries to send an unusually large number of messages, or tries to send a message to an unusually large number of recipients. This prevents your computer from being used without your knowledge to send infected attachments to other people. In addition, Outbound MailSafe protection verifies that the program attempting to send the e-mail has permission to send e-mail messages.

Outbound MailSafe protection works with any e-mail application that uses SMTP.

Enabling Outbound MailSafe protection

For your security, Outbound MailSafe Protection is enabled by default. When Outbound protection is enabled, Outbound MailSafe settings apply to all programs with send mail privileges.

To enable or disable Outbound MailSafe Protection

1. Select **E-mail Protection**.
2. In the Outbound MailSafe Protection area, select **On** or **Off**.

Customizing Outbound MailSafe protection

By default, an Outbound MailSafe protection alert is displayed when your e-mail application attempts to send more than five e-mail messages within two seconds, or if an e-mail message has more than fifty recipients. You can customize these settings to extend the time interval, increase the number of messages and recipients allowed, or specify the e-mail addresses that are allowed to send e-mail from your computer.

- Enabling Outbound MailSafe protection by program
- Setting Outbound MailSafe protection options (on page 139)

Enabling Outbound MailSafe protection by program

When Outbound MailSafe protection is set to On, protection is enabled for all programs that have been granted permission to send e-mail.

You can customize Outbound MailSafe protection by enabling or disabling it for particular programs.

For information on setting permissions for a program, see Setting permissions for specific programs (on page 111).

To enable or disable Outbound MailSafe protection for a program:

1. Select **Application Control**| **View Programs**.
2. In the Programs column, select the program name, then select **Options**.
3. Select the **Security** panel.
4. In the Outbound MailSafe Protection area, select the check box labeled **Enable Outbound E-mail Protection for this program**.

   To disable Outbound MailSafe protection, clear this check box.
5. Click **OK**.

Setting Outbound MailSafe protection options

By default, Outbound MailSafe Protection is activated when your computer attempts to send more than five e-mail messages within two seconds, or an e-mail message with more than 50 recipients.

Because even legitimate e-mail messages may have one or both of these characteristics, you may want to customize Outbound MailSafe protection settings to better meet your individual needs.

To customize Outbound MailSafe protection settings:

1. Select **E-mail Protection**, then click **Advanced**.

The Advanced E-mail Protection dialog appears.

2. In the Display Outbound MailSafe Protection Alerts When area, choose your settings.

Too many e-mails are sent at once	An Outbound MailSafe protection alert appears when your computer attempts to send more than the specified number of e-mails within the specified time interval.
A message has too many recipients	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail message with more than the specified number of recipients.
If the sender's address is not in this list	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail whose originating address (i.e., the address in the **From:** field) does not appear on the list. To prevent ZoneAlarm security software from blocking all outgoing e-mail, make sure that your valid e-mail address appears on this list.

3. Click **OK**.

Filtering junk e-mail (spam)

Use the junk e-mail filter to prevent unsolicited junk e-mail (*spam*) from cluttering your Inbox. The Junk E-mail filter supports Microsoft Outlook and Outlook Express (both referred to in this document simply as "Outlook").

During installation, the ZoneAlarmjunk e-mail filter toolbar is added to your Outlook e-mail program's toolbar.

Note - If you have installed ZoneAlarm security software but the junk e-mail filter toolbar does not appear in your Outlook toolbar, right-click in your Outlook toolbar and choose **ZoneAlarmOutlookAddin**.

The junk e-mail filter also adds three special folders to your Outlook folder list: ZoneAlarm Challenged Mail, ZoneAlarm Junk Mail, and ZoneAlarm Phishing Mail. When ZoneAlarm security software identifies an e-mail message as junk, phishing, or challenged, it puts the message in one of these folders. If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

- Allowing or blocking e-mail from specific senders, companies, or lists ("Allowing or blocking e-mail from specific senders" on page 141)
- Allowing or blocking e-mail from specific companies (on page 141)
- Adding contacts to the Allowed List (on page 141)
- Allowing e-mail from distribution lists (on page 142)
- Scanning your Inbox (on page 142)

- Reporting junk e-mail ("Reporting junk email" on page 142)
- Reporting phishing e-mail ("Reporting phishing email" on page 143)
- Specifying junk e-mail message options (on page 144)
- Challenging e-mail from unknown senders (on page 145)
- Specifying your outbound e-mail server (on page 146)
- Customizing junk e-mail filter settings ("Customizing junk email filter settings" on page 146)
- Viewing junk e-mail filter reports ("Viewing junk email filter reports" on page 148)

Allowing or blocking e-mail from specific senders

Each time you send an e-mail to a new person, the junk e-mail filter automatically adds to the Allowed list, the address in the To field. Messages sent to you from those addresses will be put in your Inbox.

When you receive an e-mail from a sender on the Blocked list, the junk e-mail filter automatically moves the message to the Outlook folder named *ZoneAlarm Junk Mail.*

If an unwanted e-mail arrives in your Outlook Inbox, you can easily add the sender of that message to your Blocked People list.

To add e-mail addresses to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender** or **Block Sender**.

Allowing or blocking e-mail from specific companies

The junk e-mail filter allows you to add all e-mail addresses originating from a particular company or network domain to your Companies Allowed or Blocked lists.

To add companies to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender's Company** or **Block Sender's Company**.

   The junk e-mail filter adds the domain portion of the sender's address (for example, *example.com*) to the list of allowed or blocked addresses.

Adding contacts to the Allowed List

You can scan the default contacts folder in your e-mail program to add contacts to the list of senders from whom you wish to receive e-mail.

To add contacts to the Allowed List:

1. Open your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Populate Allowed List**.

Scanning your Inbox

You can scan the contents of your Inbox for phishing e-mail and spam. You can use the Scan Inbox option to scan IMAP, POP3, and Hotmail accounts created in Outlook Express, and IMAP, POP3 and Exchange server accounts in Outlook.

To scan your Inbox:

1. Open your Outlook or Outlook Express e-mail program.
2. Select the Inbox you want to scan.
3. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Scan selected Inbox**.

Allowing e-mail from distribution lists

If you receive or send e-mail to multiple addressees contained in a distribution list, the junk e-mail filter may block that list name unless it has been added to the Lists panel.

To allow e-mail from mailing lists:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Lists**.
3. Click **Add**.
4. Type the e-mail address of the distribution list into the text entry area, then click **OK**.

   The junk e-mail filter adds the distribution list's e-mail address to the list of allowed addresses.
5. Click **Close** to save your changes and close the Lists panel.

Reporting junk email

The junk e-mail filter allows you to contribute instances of junk e-mail to the ZoneAlarm Collaborative Filter database.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you contribute junk e-mail to the Collaborative Filter database, you can choose to send either the actual e-mail or a digitally processed (sometimes referred to as "hashed") summary of the e-mail that removes all content, headers, and personally identifiable information from the message. Sending the entire message enables complete analysis of the contents; sending a digitally processed summary of the message ensures complete privacy.

Note - MailFrontier, a trusted ZoneAlarm partner, manages the Collaborative Filter database for ZoneAlarm. You can view the full text of MailFrontier's privacy policy at: http://www.mailfrontier.com/privacy.html

To report junk e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar:
   - To send the junk e-mail itself, click **ZoneAlarm Options**, then choose **Report Junk E-mail**.
   - To send a digitally processed summary of the junk e-mail, click **Junk**.
3. In the **Contribute E-mail** dialog box, click **OK**.

   The junk e-mail filter reports the junk e-mail to the Collaborative Filter database and moves the message to the special Outlook folder **ZoneAlarm Junk Mail**.

Note - To restore e-mail that was incorrectly identified as junk, select the e-mail in the ZoneAlarm Junk Mail folder, and click Unjunk. The e-mail will be restored to your Outlook Inbox.

Reporting phishing email

The junk e-mail filter allows you to report instances of phishing e-mail referred to as *phishing*) to ZoneAlarm. When phishing mail is detected for the first time, a popup appears, asking if you would like to send the phishing mail to ZoneAlarm for analysis. If you choose Yes, all future phishing messages will be sent without prompting you for confirmation. If you choose No, your choice will be reflected in the Configure Preferences dialog box.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you report phishing e-mail, the junk e-mail filter forwards the complete and original message to ZoneAlarm.

ZoneAlarm never divulges your e-mail address, name or other personal information contained in a phishing e-mail except as required to investigate and prosecute the originator of the phishing message.

ZoneAlarm forwards selected portions of the reported message to government and law enforcement agencies with jurisdiction over e-mail fraud. These agencies are required by law to protect the confidentiality of the information contained in the message. ZoneAlarm separately informs individuals or institutions threatened by forwarding to them only the information required to alert them.

To report phishing e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.

2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Report Phishing E-mail**.
3. In the **Contribute E-mail** dialog box, click **OK**.

   The junk e-mail filter reports the phishing e-mail to ZoneAlarm and moves the message to the special Outlook folder `ZoneAlarm Phishing Mail`. If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

Note - MailFrontier, a trusted ZoneAlarm partner, manages the processing of phishing e-mail for ZoneAlarm. You can view the full text of MailFrontier's privacy policy at: http://www.mailfrontier.com/privacy.html

Specifying junk e-mail message options

The junk e-mail filter uses three message filtering techniques: *collaborative filter*, *message filters*, and *foreign language filters*. Filter settings determine how messages are treated when received from unknown senders.

Collaborative Filter

Collaborative filtering uses information extracted from junk e-mail reported by you and other ZoneAlarm security software users to determine whether new messages received from unknown users is spam.

Message Filters

Message filters use heuristic rules to analyze e-mail for characteristics common to various types of junk e-mail.

Foreign language filters

Foreign language filters block e-mail containing non-european languages. (The junk e-mail filter automatically manages e-mail in common european languages such as French, German, or Spanish.)

To customize message filtering options:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**|**Configure Preferences** |**Messages**.

Collaborative Filter	In the area, move the slider to adjust the responsiveness to the characteristics of junk e-mail reported by other ZoneAlarm security software users.
Message Filters	Move the slider to adjust the responsiveness to common junk e-mail. You can also adjust the responsiveness to specific categories of junk e-mail.
Language Filters	In the area, click Configure then choose which languages to block.

3. Click **Close**.

Challenging e-mail from unknown senders

You can choose to have the junk e-mail filter reply to an e-mail from an unknown sender with a challenge e-mail. Because junk e-mail seldom contains a valid return address, an unanswered challenge confirms that the e-mail is probably junk.

The challenge e-mail instructs the recipient to click a button in the message to validate that he or she was the author of the message. Clicking the button directs the junk e-mail filter to move the e-mail from the special Outlook folder **ZoneAlarm Challenged Mail** folder to your Outlook Inbox.

For messages from an unknown sender, you can choose whether to always send a challenge e-mail, to send a challenge only when the incoming message appears to be junk e-mail, or to never send a challenge. In addition you can customize the challenge e-mail that is sent to users.

To enable challenge e-mails:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Challenges**.
3. In the Challenges area, use the slider to choose when to send a challenge e-mail.

High	ZoneAlarm security software will challenge all e-mails that you receive unless they are known as good to either you (on your allowed lists) or to MailFrontier (known good senders). Any e-mail message that is received and can be classified immediately as junk gets sent directly to the ZoneAlarm Mail folder for later deletion and does NOT get a challenge issued.
Low	ZoneAlarm security software will challenge uncertain e-mail. ZoneAlarm security software will only challenge e-mails that it cannot determine with certainty are spam or are good. This is typically a small percentage of the e-mail you receive.
Off	Challenge e-mails will not be sent. ZoneAlarm security software will not send challenge e-mails. Move the

	slider up to turn on e-mail challenges to eliminate junk e-mail sent by spammer computers.

4. To add a personal message to the standard challenge e-mail, click **Personalize**, type your name and your personal message, then click **OK**.
5. Click **Close**.

   The junk e-mail filter moves the message to the **ZoneAlarm Challenged Mail**. folder

Important - While waiting for the response to a challenge message, the junk e-mail filter stores your e-mail address. As soon as the challenge has been completely processed, the junk e-mail filter discards the address. If you experience problems sending challenge e-mails, see Specifying your outbound e-mail server (on page 146).

Specifying your outbound e-mail server

To send challenge e-mails, the junk e-mail filter requires the ability to send e-mail. In most cases the junk e-mail filter uses Outlook's default outbound mail server. If you experience problems sending challenge e-mails, you may need to specify the name of your outbound e-mail server.

To specify the name of an outbound e-mail server:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**|**Configure Preferences** |**Challenges**.
3. In the Challenge Content area, click **E-mail Server**.
4. Type the name of your outbound e-mail server, then click **OK**.
5. Click **Close**.

Customizing junk email filter settings

By default, the junk e-mail filter retains phishing e-mail messages in the **ZoneAlarm phishing Mail** folder until you manually delete them. You can specify how long e-mail messages are stored in the **ZoneAlarm Junk Mail** and **ZoneAlarm Challenged Mail** folders, as well as automate fraud e-mail reporting, and configure wireless device forwarding. In addition, if you could like to scan more than one Outlook Inbox, you can specify those settings here.

To specify storage duration for junk e-mail:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**|**Configure Preferences** |**Settings**.
3. In the Junk Folder Settings area, click **Configure**.
4. Type the number of days to retain suspected junk e-mail in the **ZoneAlarm Junk Mail** and **ZoneAlarm Challenged Mail** folders.

The junk e-mail filter moves e-mail that has been in the folder for the specified number of days without being validated into Outlook's Deleted Items folder.

5. Click **Close**.

To configure a wireless device:

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Wireless Device Support area, click **Configure**.
4. In the **ZoneAlarm Wireless Support** dialog box, type the e-mail address of your wireless device.

   You can also choose to forward only e-mail headers, and to specify the number of validate messages forwarded to your wireless device in a 24-hour period.
5. If you need to specify a non-default e-mail server, click **E-mail Server**, type the name of your outbound e-mail server, then click **OK**.

   Click **Close** to save your changes.

To enable automatic reporting of phishing e-mail:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Auto Report Fraud E-mail area, select the **Enable auto reporting...** check box.
4. Click **Close.**

To customize confirmation messages:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Show Confirmations area, specify the settings you want.

Contribute Junk Email	Displays an alert prior to sending junk e-mail to ZoneAlarm.
Contribute Phishing Email	Displays an alert prior to sending phishing e-mail to ZoneAlarm.

4. Click **Close**.

To configure multiple Outlook inboxes:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Outlook Multiple Inbox Support area, select the check box **Support scanning of multiple Inbox in Microsoft Outlook**.

Note - This feature is enabled by default.

Restoring e-mail incorrectly identified as junk

The junk e-mail filter adds three special folders to your Outlook folder list: **ZoneAlarm Challenged Mail**, **ZoneAlarm Junk Ma**il, and **ZoneAlarm Phishing Mail**. When ZoneAlarm security software identifies an e-mail message as junk, fraudulent, or challenged, it puts the message in one of these special folders.

If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

You can restore mail that the junk e-mail filter incorrectly placed in a special folder to your Outlook Inbox.

To restore e-mail incorrectly identified as junk:

1. In your Outlook or Outlook Express e-mail program, in the **ZoneAlarm Challenged Mail**, **ZoneAlarm Junk Mail**, or **ZoneAlarm Phishing Mail** folder, choose an e-mail.
2. In the junk e-mail filter toolbar, click **Unjunk**.

   The junk e-mail filter restores the selected message to your Outlook Inbox.

Viewing junk email filter reports

Use the junk e-mail filter's Reports panel to view a summary of mail processing activity.

To view junk e-mail filter reports

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Reports**.
3. Choose one of the four report types:

Junk by Day	The total number of legitimate and junk e-mails received by day.
Reasons	The reasons the junk e-mail filter blocked incoming e-mails by day
Total History Junk by Day	The total number of legitimate and junk e-mails received since ZoneAlarm security software was installed.
Total Reasons	The total number of reasons the junk e-mail filter blocked incoming e-mails since ZoneAlarm security software was installed.

4. Click **Close** to close the Reports panel.

With the rise of e-commerce, electronic record keeping, and mass financial mailings, the incidence of identity theft increased. Hackers can use malware to intercept your personal information online, while thieves can steal CDs and laptops containing customer information, or they can intercept sensitive mail items (such as pre-approved credit card offers) that include personal data.

ZoneAlarm security software helps protect your personal data online and out in the everyday world. ID Lock keeps your personal information safe from hackers and identity thieves.

Understanding the ID Lock feature

Every time you or someone else using your computer enters personal information into an e-mail message or Web form—such as your credit card number, address, or social security number— it is possible that the information could be stolen. To help prevent that from happening, the ID Lock ensures that your personal information is only sent to sites you trust.

The ID Lock feature provides a secure area called myVAULT, where you can store personal information that you want to protect. The contents of myVAULT are blocked from being transmitted to unauthorized destinations, whether by you, someone else using your computer, or by a Trojan horse attempting to transmit your personal information.

- How your personal information is protected (on page 149)
- Setting the ID Lock protection level (on page 151)

How your personal information is protected

ZoneAlarm security software prevents your personal information from being transmitted without your authorization, whether in e-mail or on the Web.

E-mail transmission

When you or someone using your computer attempts to send myVAULT data in an e-mail message, ZoneAlarm security software displays an alert asking you whether to allow the information to be sent. If you want to always allow or always block the information from being sent to this destination, before clicking Yes or No select the check box labeled **"Do you want to remember this answer..."** to add the destination to your Trusted Sites list with the corresponding permission set automatically. For example, if you were to select the "Do you want to remember this answer..." check box and then click **Yes**, the destination would be added to the Trusted Sites list with the permission set to **Allow**. Conversely, if you were to click **No**, the permission would be set to **Block**.

Important - When responding to an ID Lock alert that is the result of an e-mail transmission, clicking the **"Do you want to remember this answer..."** check box adds the domain of the intended recipient's e-mail server—not the e-mail recipient—to the Trusted Sites list. For

example, if you were to allow myVAULT data to be transmitted to your contact john@example.com, and you chose to remember that answer, the next time myVAULT data is sent to ANY contact on example.com's e-mail server, the transmission would be allowed and you would not see an alert.

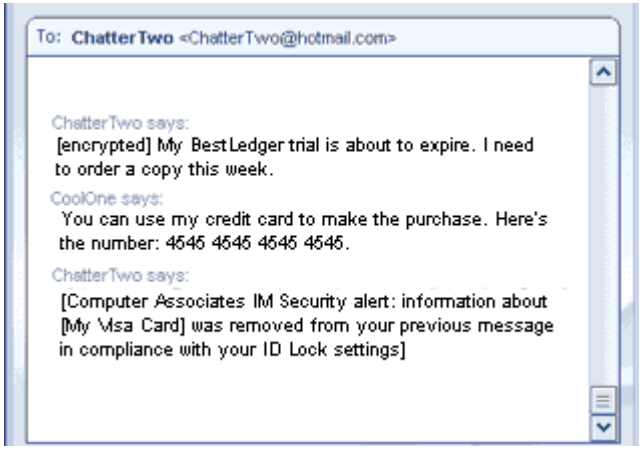
Web transmission

When transmitting myVAULT data on the Web, ZoneAlarm security software allows or blocks the transmission according to the permission for the domain in the Trusted Sites list. As with e-mail transmission of myVAULT contents, if you choose to remember your response to an ID Lock alert for a particular Web site, that Web site will be added to the Trusted Sites list automatically with the permission set accordingly.

IM transmission

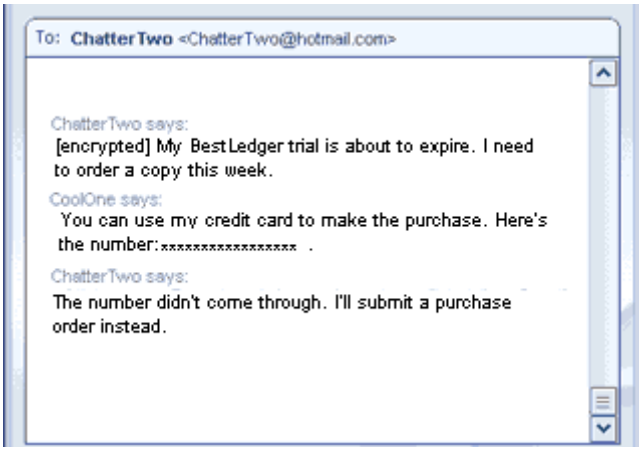
When transmitting myVAULT data in an Instant Messaging conversation, ZoneAlarm security software prevents the information from being received.

The picture below shows an instant messaging conversation in which information that is stored in myVAULT is transmitted. The description of the item stored in myVAULT (in this example, My Visa Card) appears in brackets.


To: ChatterTwo <ChatterTwo@hotmail.com>
ChatterTwo says:
[encrypted] My BestLedger trial is about to expire. I need to order a copy this week.
CoolOne says:
You can use my credit card to make the purchase. Here's the number: 4545 4545 4545 4545.
ChatterTwo says:
[Computer Associates IM Security alert: information about [My Visa Card] was removed from your previous message in compliance with your ID Lock settings]

Transmission of myVAULT contents

The picture below shows how the transmitted information is displayed to the recipient. The protected information is replaced with asterisks so that it is unreadable.


To: ChatterTwo <ChatterTwo@hotmail.com>
ChatterTwo says:
[encrypted] My BestLedger trial is about to expire. I need to order a copy this week.
CoolOne says:
You can use my credit card to make the purchase. Here's the number:**********.
ChatterTwo says:
The number didn't come through. I'll submit a purchase order instead.

Receipt of myVAULT contents

Setting the ID Lock protection level

The ID Lock is disabled by default. By enabling the ID Lock, you ensure that the data entered in myVAULT will be protected.

ZoneAlarm security software keeps track of the number of items stored in myVAULT and displays the number of times your information was protected.

To set the ID Lock protection level:

1. Select **Identity Protection**.
2. In the Identity Lock area, specify the desired protection level.

High	Prevents the contents of myVAULT from being sent to unauthorized destinations. ZoneAlarm security software will block transmission of your data silently. If you are using a shared computer, this setting is recommended for maximum security.
Medium	Alerts you when your identity information is about to be sent to destinations not listed on the Trusted Sites list. This is the default setting.
Off	Identity protection is disabled. The contents of myVAULT can be sent to any destination, whether or not it appears on the Trusted Sites list.

About myVAULT

The myVAULT feature provides a secure area for entering your critical personal data—data that you want to protect from hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, ZoneAlarm security software determines whether the information should be blocked or allowed. By default, ZoneAlarm security software encrypts myVAULT data as it is entered, storing only the hash value of the data rather than the data itself. Encrypting the data keeps your information secure, as data cannot be retrieved using the hash value.

- Adding data to myVAULT (on page 152)
- Editing and removing myVAULT contents (on page 154)

Adding data to myVAULT

While you can store any type of information in myVAULT, it is a good idea only to store information that you wish to keep secure, such as credit card numbers and identification information. If you were to store information such as your country of residence (for example, Canada) in myVAULT separately from the rest of your address, any time you typed "Canada" into an online Web form, ZoneAlarm security software would block transmission of the data.

Note - If you're unsure of the type of information that should be entered into myVAULT, refer to the pre-defined categories for guidance. To access the list of categories, select **Identity Protection** | **myVAULT**, then click **Add**.

To add information to myVAULT:

1. Select **Identity Protection|myVAULT**.
2. Click **Add**.

   The Add information to myVAULT dialog box will appear.

   For maximum protection, ZoneAlarm security software encrypts myVAULT data by default. If you do not want to encrypt the data as you enter it, clear the **Use one-way encryption**... check box.
3. Type a description of the item you are adding.

   Important - ZoneAlarm security software displays the item description in ID Lock alerts. Be sure that the description you enter is different from the value of the item to be protected. If the information to be protected and the description contain some or all of the data, you may receive multiple ID Lock alerts.
4. Select a category from the drop-down list.

Access PIN	Personal access code or other ID number. Maximum of 6 characters. For added security, Access PINs are always encrypted.

Address	Maximum 30 characters.
American Express card	For added security, ZoneAlarm security software does not record the last 5 digits of your American Express card number.
Bank account	Maximum 14 characters.
Credit card	For added security, ZoneAlarm security software does not record the last 4 digits of your credit card number.
Driver's license	Maximum 15 characters.
eBay password	The password you use to access the eBay Web site. Your eBay password can only be sent to eBay. Maximum 20 characters.
E-mail Address	Maximum 60 characters.
International tax ID	Maximum 15 characters.
Mother's maiden name	Maximum 30 characters.
Name	Maximum 30 characters.
Passport number	US passport number or other International ID number. Maximum 30 characters.
Password	Enter the password to be protected. Maximum 20 characters.
Phone	Separators such as parentheses and dashes are not allowed. Maximum 13 characters.
US Social Security number	Requires 9 digits.
Other	Use this field to enter items that either do not correspond to any of the pre-configured categories, or which exceed the character limit for the corresponding category. Maximum 30 characters.

5. Type the data to be protected.

Note - Data encryption is enabled by default. If you do not want to encrypt your data, clear the **Use one-way encryption...** check box. Because of the sensitive nature of the data, PIN numbers, passwords, the last four digits of your social security number, and the last four digits

of your credit card numbers will always be displayed as asterisks, whether or not you choose to encrypt them.

To disable the encryption confirmation that appears by default, select **Identity Protection** | **myVAULT**, then click **Options**. Clear the **Show encryption confirmation** check box.

Asterisks will appear in place of the data you entered and an encrypted form of your data will be stored in myVAULT. ZoneAlarm security software will compare the encrypted data with your outgoing messages.

6. Specify whether you want the information to be protected when using Web, E-mail, and Instant Messengers (if available in your version of the product).
7. Click **OK** to save your changes.

Editing and removing myVAULT contents

In the myVAULT panel you can modify the encryption setting, remove myVAULT contents, and edit unencrypted data. Because encrypted data is displayed in asterisks, it is unreadable and therefore cannot be edited.

To edit myVAULT contents:

1. Select **Identity Protection**|**myVAULT**.
2. Select the item you want to edit, then click **Edit**.

   The Edit information from myVAULT dialog appears.
3. Modify data as necessary, then click **OK** to save your changes.

To remove myVAULT contents:

Select the item you want to remove, then click **Remove**.

Note - If you remove the last item in myVAULT, the ID Lock protection level will be set to Off. If you later add items to myVAULT, the protection level will be reset to the default Medium setting.

Using the Trusted Sites list

The myVAULT feature provides a secure area for entering your critical personal data—data that could be used by hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, ZoneAlarm security software determines whether the information should be blocked or allowed, by making sure the destination is one you trust.

There are two kinds of sites that can appear on the Trusted Sites list: Security Alliance and Custom. Security Alliance sites are sites that ZoneAlarm has authenticated to ensure they are not fraudulent. Custom sites are sites you add to the list.

Viewing the Trusted Sites list

In addition to listing sites you trust with your personal information, you can add sites to the list that you explicitly do *not* want to trust, such as known spam or chat sites, and prevent information from being sent to them.

To see the Trust Sites list, select **IDENTITY & DATA** | **View Trusted Sites**.

The Trusted Sites list also lets you specify which sites are allowed to send your password as *clear text*. Because clear-text passwords are unencrypted, they can easily be viewed by others if intercepted during transmission.

Access permission

Specifies whether ZoneAlarm security software will allow, block, or alert you before sending myVAULT contents to the listed destinations. To modify the permission for a site, click beside the site in the Access column and choose **Allow, Block**, or **Ask**.

Site

Displays the domain of the site.

Type

Specifies whether the site is a Security Alliance partner or a Custom site.

Clear Text password

Specifies whether ZoneAlarm security software will allow, block, or alert you before sending your password as clear text to the listed destinations. To modify the permission for a site, click beside the site in the Clear Text password column and choose **Allow, Block**, or **Ask**.

Site Entry Details

In addition to the site name and type, the Entry Details box displays the site IP Address and the date and time you last accessed the site.

Adding to the Trusted Sites list

There are two types of sites that appear on the Trusted Sites list: Custom and Security Alliance. Custom sites are sites that you add to the list. Security Alliance partner sites are sites that ZoneAlarm has verified are legitimate and has added automatically.

Custom sites are trusted at the domain level, therefore each sub-domain you want to trust must be added separately. For example, www.msn.com and shopping.msn.com would need to be

added separately. Security Alliance sites explicitly trust all sub-domains, so you do not need to create an entry for each sub-domain you want to trust.

To add a site to the Trusted Sites list:

1. Select **Identity Protection**|**Trusted Sites**, then click **Add**.

   The Add Trusted Site dialog appears.
2. Type the URL of the site (omit http://www), then click **OK**.

   After you click OK, ZoneAlarm security software verifies the site address and records the IP address. This process can take several seconds.
3. Modify the site permissions as desired.

   By default, access and clear text password permissions for Custom sites are set to Ask.

Editing and removing trusted sites

In the Trusted Sites panel, you can modify the access permission for a site, and edit or remove Custom sites. Although you can modify the permissions for Security Alliance partner sites, you cannot edit or remove the site entry.

To edit a Custom site:

1. Double-click the site you want to edit.

   The Edit trusted site dialog appears.
2. Edit the site as necessary, then click **OK** to save your changes.

To remove a custom site:

Right-click the site you want to remove, then click **Remove**.

Identity Protection Center (US only)

The ZoneAlarm Identity Protection Center is a Web site that helps you prevent, detect, and, if necessary, recover from identity theft. (Identity theft is a crime in which someone exploits your personal information for their own gain.) The Identity Protection Center includes identity protection tips as well as resources for monitoring the use of your personal information and for recovering from identity theft.

To visit the Identity Protection Center:

1. Go to **Identity Protection**.
2. In the Identity Protection Center area, click **Go to ZoneAlarm Identity Protection Center**.

Encrypting your hard drive is important because if your computer is lost or stolen, a hacker can remove your drive and read it without even knowing your Windows logon name and password. But, if your drive is encrypted, your sensitive data is protected--thieves are locked out of it.

What Hard Drive Encryption does for you

Hard Drive Encryption makes everything on your computer unreadable to unauthorized users. Your own encryption password is required before your computer fully boots up.

Your full hard disk is encrypted, including deleted and temporary files, which protects your sensitive data if your disk is stolen or lost. This prevents hackers from breaking into your operating system by removing your disk and using bypass tools or alternative boot media.

DataLock hard drive encryption is ideal for:

- anyone who has identity information, such as tax forms or financial account data, on their computer and thinks there is a risk of their computer being lost or stolen (e.g., while traveling or in public places)
- small business owners and others who have proprietary or private data, such as client files, on their computer

Installing ZoneAlarm DataLock

If you have a license that supports ZoneAlarm DataLock, and it is not yet installed, you can install it from the ZoneAlarm window.

To install ZoneAlarm DataLock:

1. Back up copies of your valued files.
2. On the ZoneAlarm **IDENTITY & DATA** panel, click **Install** next to Hard Drive Encryption.
3. The installation wizard appears and steps you through:
    - Creating an account for support, and then one for logging in to ZoneAlarm DataLock.
    - Installation and restart.

About encryption after installation

Encryption starts automatically and runs in the background. It may take a few hours for full encryption to complete. You can use your computer and turn it on and off during this process. Encryption pauses while your computer is off.

Using ZoneAlarm DataLock

After installation and recovery disk creation, all you need to do is memorize your ZoneAlarm DataLock login credentials and keep them secret. You will need them each time you start up your computer.

How it affects your day-to-day computer usage:

- **Another login at startup:** Before your Windows login screen appears, you log in to a ZoneAlarm DataLock screen when you start your computer. This gives you secure access to your encrypted operating system.
- **The rest is silent and invisible:** Your files and desktop are silently decrypted when you access them and encrypted when you close them, but this process is invisible to you.

Hard Drive Encryption automatically encrypts all internal hard drives, but does not encrypt any external hard drives.

About the DataLock Settings Panel

The **DataLock Hard Drive Encryption | Settings** panel in shows the progress and completion of encryption after you install DataLock.

Encryption takes place in the background and does not affect your system experience. While individual files and your desktop are invisibly decrypted on access and encrypted when you close them, the Encryption Status bar maintains a 100% status to indicate you have full encryption protection.

Stopping or uninstalling ZoneAlarm DataLock

There is no on or off button for DataLock, but you can uninstall it by clicking the **Uninstall** button on the **IDENTITY & DATA | DataLock Hard Drive Encryption | Settings** panel.

Decryption may take a few hours, and will require you to restart your computer. ZoneAlarm DataLock will be completely uninstalled after decryption completes.

You can use your computer and turn it on and off during this decryption, though decryption pauses when your computer is off.

Troubleshooting ZoneAlarm DataLock

In addition to the Troubleshooting topics below, see Stopping or uninstalling ZoneAlarm DataLock (on page 158).

What to do if you forget your password or username

If you forget your ZoneAlarm DataLock login credentials:

- Click the **Help** button on the ZoneAlarm DataLock login screen. Use the contact information that appears.

- We will authenticate your identity with the security questions you created during installation, and help you regain access to your computer.

Tip:	By default, your username is the same as your Windows logon username.

How to decrypt in case of system failure

If a system crash locks you out of access to your login screen, you can decrypt your drive in order to recover your files.

To decrypt when you need to recover your data:

1. Locate the recovery disk you created at installation (it would be on a CD or USB stick). If you don't have it, just contact Support (http://www.zonealarm.com/support) for help. Support has your recovery information because it's automatically uploaded during installation.
2. Insert the recovery disk and restart your computer.
3. Follow the instructions that appear.
   - Because it is a pre-boot environment, use the **Tab** key to move the cursor and press **Enter** to make a selection. (The mouse won't work.)
   - Once decryption starts, the percentage of the decryption is displayed. It can take up to a few hours to complete.
   - When decryption is complete, you'll be prompted to reboot.
4. Be sure to eject the recovery disk before you power back up.

Note - After you power down, eject the recovery disk, otherwise you'll be booted into the recovery environment again.

To reactivate ZoneAlarm DataLock, you need to remove it. See Stopping or removing ZoneAlarm DataLock, Then, reinstall it.

Managing Alerts and Logs

Whether you're the type of person who wants to know everything that happens on your computer—or you only want to know that your computer is secure, ZoneAlarm security software accommodates you. You can be notified by an alert each time ZoneAlarm security software acts to protect you, or only when an alert is likely to have resulted from hacker activity. You can also choose to log all alerts, only high-rated alerts, or alerts caused by specific traffic types.

Note - For information about suppressing most alerts while playing

games on your computer, see Game Mode (on page 168).

Understanding alerts and logs

Understanding and reducing alerts

To learn about the various kinds of ZoneAlarm security software alerts you may see, see Understanding and reducing alerts (on page 46).

Understanding the alerts and logs panel

ZoneAlarm security software alert and logging features keep you aware of what's happening on your computer without being overly intrusive, and enable you to go back at any time to investigate past alerts.

Expert rule options let you track not only blocked Internet traffic, but allowed traffic as well, giving advanced users the option of maximum information for customizing security rules for their environment.

About event logging

By default, ZoneAlarm security software creates a log entry every time traffic is blocked, whether an alert is displayed or not. Log entries record the traffic source and destination, ports, protocols, and other details. The information is recorded to a text file named ZALOG.txt, stored in the Internet Logs folder. Every 60 days, the log file is archived to a dated file so that it doesn't become too large.

You can choose to prevent specific categories of events from being logged—for example, you may want to create log entries only for firewall alerts, or suppress entries for a particular type of Program alert. You can also have ZoneAlarm security software log specific types of traffic you have decided to allow, by creating expert rules with tracking features enabled.

Showing or hiding firewall and program alerts

The Alert Events panel gives you more detailed control of alert display by allowing you to specify the types of blocked traffic for which Firewall and Program alerts are displayed.

To show or hide firewall or program alerts:

1. Select **Tools** | **Logs.**
2. Select the **Alert Events** panel.

3. In the Alert column, select the type of blocked traffic for which ZoneAlarm security software should display an alert.
4. Click **Apply** to save your changes.

Setting basic alert and log options

Basic alert and log options let you specify the type of event for which ZoneAlarm security software displays an alert and for which events it creates a log entry.

- Setting the alert event level
- Setting event and program logging options

Setting the alert event level

The Alert Events Shown control, in the main panel of Alerts & Logs, lets you control the display of alerts by rating. Program and ID Lock alerts are always displayed, because they ask you to decide whether to grant permission.

To set the alert event level:

1. Select **Tools | Logs**.
2. In the Alert Events Shown area, select the desired setting.

High	Displays an alert for every security event that occurs, both high-rated and medium-rated.
Med	Displays only high-rated alerts, which are most likely a result of hacker activity.
Off	Displays Program and ID Lock alerts only. Informational alerts are not displayed.

Setting event and program logging options

Use the Event Logging and Program Logging areas to choose what types of informational alerts and program alerts will be logged.

To enable or disable event logging and program logging:

1. Select **Tools | Logs**.
2. In the Event Logging area, select the desired setting.

On	Creates a log entry for all events.

Off	No events are logged.

3. In the Program Logging area, specify the log level.

High	Creates a log entry for all program alerts.
Med.	Creates a log entry for high-rated program alerts only.
Off	No program events are logged.

Controlling the number of alerts

You can specify whether you want to be alerted to all security and program events, or if you only want to be notified of events that are likely a result of hacker activity.

- If you want to suppress most alerts while playing a computer game, see Game Mode (on page 168).
- For details about how to reduce certain types of alerts, and why each alert happens, see Understanding and reducing alerts (on page 46).

Showing or hiding firewall and program alerts

The Alert Events panel gives you more detailed control of alert display by allowing you to specify the types of blocked traffic for which Firewall and Program alerts are displayed.

To show or hide firewall or program alerts:

1. Select **Tools** | **Logs.**
2. Select the **Alert Events** panel.
3. In the Alert column, select the type of blocked traffic for which ZoneAlarm security software should display an alert.
4. Click **Apply** to save your changes.

Setting event and program log options

You can specify whether ZoneAlarm security software keeps record of security and program events by enabling or disabling logging for each type of alert.

- Formatting log appearance
- Customizing event logging
- Customizing program logging

- Viewing log entries
- Viewing the text log
- Archiving log entries

Formatting log appearance

Use these controls to determine the field separator for your text log files.

To format log entries:

1. Select **Tools | Logs**, then click **Log Control**.
2. In the Log Archive Appearance area, select the format to be used for logs.

Tab	Select Tab to separate fields with a tab character.
Comma	Select Comma to separate fields with a comma.
Semicolon	Select Semicolon to separate log fields with a semicolon.

Customizing event logging

By default, ZoneAlarm security software creates a log entry when a high-rated firewall event occurs. You can customize Firewall alert logging by suppressing or allowing log entries for specific security events, such as MailSafe quarantined attachments, Blocked non-IP packets, or Lock violations.

To create or suppress log entries based on event type:

1. From the Tools menu, choose **Logs**.
2. Select **Alert Events**.
3. In the Log column, select the type of event for which ZoneAlarm security software should create a log entry.
4. Click **Apply** to save your changes.
5. Click **OK**.

Customizing program logging

By default, ZoneAlarm security software creates a log entry when any type of Program alert occurs. You can customize Program alert logging by suppressing log entries for specific Program alert types, such as New Program alerts, Repeat Program alerts, or Server Program alerts.

To create or suppress log entries based on event type:

1. Select **Tools** | **Logs**.
2. In the **Program Logging** area, click **Custom**.

3. In the Program Logs column, select the type of event for which ZoneAlarm security software should create a log entry.
4. Click **Apply** to save your changes.
5. Click **OK** to close the Alert & Log Settings dialog.

Viewing log entries

You can view log entries two ways: in a text file using a text editor, or in the Log Viewer. Although the format of each type of log differs slightly, the general information contained in the log is the same.

To view the current log in the Log Viewer:

1. Select **Tools** | **Logs**| **Log Viewer**.
2. Select the number of alerts to display (from 1 to 999) in the alerts list.

   You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.
3. Select the type of alert you want to view:

Anti-virus	Displays the Date/Time, Type, Virus Name, File Name, Action Taken, Mode, and E-mail Info columns.
Firewall	Displays the Rating, Date/Time, Type, Protocol, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.
OSFirewall	Displays the Rating, Date/Time, Type, Subtype, Data, Program, Direction, Action Taken, and Count columns.
Program	Displays the Rating, Date/Time, Type, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.

Note - The Log Viewer shows security events that have been recorded in the ZoneAlarm security software log. To view details of Log Viewer fields for each alert type, refer to the Firewall, Application Controll, and Anti-virus chapters.

Field	Information
Description	A description of the event.
Direction	The direction of the blocked traffic. "Incoming" means the traffic was sent to your computer. "Outgoing" means the traffic was sent

Field	Information
	from your computer.
Source DNS	The domain name of the computer that sent the traffic that caused the alert.
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm security software blocked.
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Protocol	The communications protocol used by the traffic that caused the alert.
Action Taken	How the traffic was handled by ZoneAlarm security software.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.
Destination IP	The address of the computer the blocked traffic was sent to.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Date/Time	The date and time the alert occurred.
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).

Log viewer fields

Viewing the text log

By default, alerts generated by ZoneAlarm security software are logged in the file, *ZAlog.txt*. If you are using Windows95, Windows98 or Windows Me, the file is located in the following folder: (x):\Windows\Internet Logs. If you are using WindowsNT or Windows2000, the file is located in the following folder: (x):\Winnt\Internet Logs.

To view the current log as a text file:

1. Select **Tools | Logs**.
2. Select the **Log Control** panel.
3. In the Log Archive Location area, click **View Log**.

Text log fields

Log entries contain some combination of the fields described in the table below.

Field	Description	Example
Type	The type of event recorded.	FWIN
Date	The date of the alert, in format yyyy/mm/dd	2001/12/31(December 31, 2001)
Time	The local time of the alert. This field also displays the hours difference between local and Greenwich Mean Time (GMT).	17:48:00 -8:00GMT (5:48 PM, eight hours earlier than Greenwich Mean Time. GMT would be 01:48.)
Virus Name	The name of the virus that caused the event. This field only appears for anti-virus events.	iloveyou
File name	The name of the file that caused the event. This field only appears for Anti-virus events.	iloveyou.exe
Action	How the event was handled. The value for this field will depend on the type of event that occurred.	Anti-virus: Renamed MailSafe: Quarantined ID Lock: Blocked
Category	The ID Lock category of information that was detected in the event. This field only appears for ID Lock events.	Access PIN
Program	The program sending or receiving the e-mail that contains the ID Lock information. This field only appears for ID Lock events.	Outlook.exe
Source	The IP address of the computer that sent the blocked packet, and the port used; OR the program on your computer that requested access permission.	192.168.1.1:7138 Outlook.exe
Destination	The IP address and port of the computer the blocked packet was addressed to.	192.168.1.101:0

Field	Description	Example
Transport	The protocol (packet type) involved.	UDP

Archiving log entries

At regular intervals, the contents of ZAlog.txt are archived to a date-stamped file, for example, ZALog2004.06.04.txt (for June 4, 2004). This prevents ZAlog.txt from becoming too large.

To view archived log files, use Windows Explorer to browse to the directory where your logs are stored.

To set archive frequency:

1. Select **Tools | Logs**.
2. Select the **Log Control** panel.
3. Select the **Log Archive Frequency** check box.

Note - If the Log Archive Frequency check box is not selected, ZoneAlarm security software continues to log events for display in the Log Viewer panel, but does not archive them to the ZAlog.txt file.

4. In the Log Frequency area, specify the log frequency (between 1 and 60 days), then click **Apply**.

Specifying the archive location

The ZAlog.txt file and all archived log files are stored in the same directory.

To change the log and archive location:

1. Select **Tools | Logs**.
2. Select the **Log Control** panel.
3. In the Log Archive Location area, click **Browse**.

   Select a location for the log and archive files.

Using SmartDefense Advisor and Hacker ID

ZoneAlarm SmartDefense Advisor is a service that enables you to instantly analyze the possible causes of an alert, and helps you decide how to respond. When available, SmartDefense Advisor provides advice as to how to respond to Program alerts. If no advice is available, click **More Info** in the alert to receive more information about the alert. SmartDefense Advisor returns an article

that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

To determine the physical location and other information about the source IP address or destination IP address in an alert, click the Hacker ID panel. This panel displays available information about the IP address that was submitted.

To submit an alert to SmartDefense Advisor:

1. Select **Tools | Logs** | **Log Viewer**.
2. Right-click anywhere in the alert record you want to submit.
3. Select **More Info** from the shortcut menu.

Game Mode

Game Mode temporarily suppresses most ZoneAlarm security software scans, product updates, and alerts, so that you can play games on your computer with fewer interruptions.

Understanding Game Mode

Game Mode minimizes interruptions while you play computer games by doing the following:

- Lets you temporarily allow or deny all program permission requests, so that requests are answered without displaying alerts.
- Postpones automatic scans and product updates.
- Suppresses all Informational alerts and all alerts in which you are prompted to make a decision. This includes:
  - Alerts caused by Ask settings in the Programs List, such as permission alerts triggered by programs trying to send mail or act as servers.
  - OSFirewall alerts, which prompt you to allow or deny behavior considered unusual or suspicious.
  - ID Lock alerts and Outbound Mailsafe alerts.

Game Mode settings do not override Block or Allow settings in your Programs List. If you have configured ZoneAlarm security software to always block a specific program, it continues to block that program even if you activate Game Mode with a setting of Allow.

Game Mode remains active until you turn it off, or until you turn off ZoneAlarm security software or your computer.

See Turning Game Mode On and Off.

Turning Game Mode On and Off

To turn Game Mode on:

1. Do one of the following:
   - In ZoneAlarm, choose **Tools | Game Mode.**
   - Or, right-click the ZoneAlarm notification tray icon and choose **Game Mode...**
2. In the dialog that appears, choose one of the following:

   Answer all alerts with "allow"—Permission requests will be granted.

   Answer all alerts with "deny"—Permission requests will be denied.

   See Understanding Game Mode (on page 168) for more information.

   Important - The use of Game Mode may reduce the security of your system. If you choose to allow all permission requests, you may increase the chances of a malicious program harming your computer or gaining access to your data. If, on the other hand, you choose to deny all requests, you may interrupt the functions of a legitimate program.

   You should activate Game Mode only for the duration of your game.

3. Leave the Activate Game Mode dialog open or minimize it, but do not close it.

   Important - If you close the Activate Game Mode dialog, you turn Game Mode off.

   While Game Mode is on, ZoneAlarm security software displays a special notification icon in the lower left corner of your screen.

To turn Game Mode off:

1. Do one of the following:
   - Close the Activate Game Mode dialog by clicking either **Cancel** or the Close icon (x) at upper right.
   - Click **Stop Game Mode** in the Activate Game Mode dialog.
   - Right-click the notification icon and choose **Stop Game Mode**.

Note that Game Mode is automatically deactivated if you turn off your computer or if you turn off ZoneAlarm security software.

Troubleshooting

Troubleshooting VPN

If you are having difficulty using VPN software with ZoneAlarm security software, refer to the table for troubleshooting tips provided in this section.

If...	See...
You can't connect to your Virtual Private Network (VPN)	Configuring ZoneAlarm security software for VPN traffic (on page 170)
You have created expert firewall rules	VPN auto-configuration and expert rules (on page 171)
You are using a supported VPN client and ZoneAlarm security software does not detect it automatically the first time you connect	Automatic VPN detection delay (on page 171)

Troubleshooting VPN problems

Configuring ZoneAlarm security software for VPN traffic

If you cannot connect to your VPN, you may need to configure ZoneAlarm security software to accept traffic coming from your VPN.

To configure ZoneAlarm security software to allow VPN traffic:

1. Add VPN-related network resources to the Trusted Zone.

   See Adding to the Trusted Zone (on page 30).
2. Grant access permission to the VPN client and any other VPN-related programs on your computer.

   See Setting permissions for specific programs (on page 111).
3. Allow VPN protocols.

   See Adding a VPN gateway and other resources to the Trusted Zone (on page 22).

VPN auto-configuration and expert rules

If you have created expert firewall rules that block VPN protocols, ZoneAlarm security software will not be able to automatically detect your VPN when you initiate a connection. To configure your VPN connection, you will need to make sure that your VPN client and VPN-related components are in the Trusted Zone, and that they have permission to access the Internet. See Configuring your VPN connection (on page 20).

Automatic VPN detection delay

ZoneAlarm security software periodically polls your computer to determine if supported VPN protocols are engaged. Upon detection, ZoneAlarm security software prompts you to configure your connection automatically. If you have recently install a VPN client and have tried to connect, ZoneAlarm security software may not have detected your VPN configuration. If you prefer ZoneAlarm security software to configure your connection automatically, you can wait ten minutes then, try connecting again. If you prefer to connect right away, you can configure your connection manually. See Configuring your VPN connection (on page 20).

Troubleshooting networking

If you are having difficulty connecting to your network or using networking services, refer to the table for troubleshooting tips provided in this section.

If ...	See...
You can’t see the other computers in your Network Neighborhood, or if they can’t see you	Making your computer visible on your local network (on page 171)
You can’t share files or printers over your home or local network	Sharing files and printers across a local network (on page 172)
Your computer is on a Local Area Network (LAN) and takes a long time to start up when ZoneAlarm security software is installed	Resolving a slow start up (on page 172)

Troubleshooting network problems

Making your computer visible on your local network

If you can’t see the other computers on your local network, or if they can’t see your computer, it is possible that ZoneAlarm security software is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible on the local network:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See Adding to the Trusted Zone (on page 30).
2. Set the Trusted Zone security level to Medium, and the Public Zone security level to High. This allows trusted computers to access your shared files, but blocks all other machines from accessing them. See Setting advanced security options (on page 26).

Note - ZoneAlarm security software will detect your network automatically and display the New Network wizard that lets you add your network subnet to the Trusted Zone.

Sharing files and printers across a local network

ZoneAlarm security software enables you to quickly and easily share your computer so that the trusted computers you're networked with can access your shared resources, but Internet intruders can't use your shares to compromise your system.

To configure ZoneAlarm security software for secure sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See Adding to the Trusted Zone (on page 30).
2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files. See Choosing security levels (on page 25).
3. Set the Public Zone security level to High. This makes your computer invisible to non-trusted computers. See Setting the security level for a Zone (on page 25).

Resolving a slow start up

If ZoneAlarm security software is configured to load at startup, some users connected to the LAN may find that it takes several minutes for the startup process to finish.

In most cases, this is because your computer needs access to your network's Domain Controller to complete its startup and login process, and ZoneAlarm security software is blocking access because the Controller has not been added to the Trusted Zone.

To solve this problem, add the host name or IP address of your network's Domain Controller to the Trusted Zone.

Troubleshooting an Internet disconnection

If you are having difficulty connecting to the Internet, first see whether ZoneAlarm is related to your Internet disconnection by trying to connect when ZoneAlarm is off:

1. Right-click the ZoneAlarm icon in the Windows taskbar notification area and choose **Shutdown**... .
2. Can you connect with ZoneAlarm off?
   - **If no (you cannot connect when ZoneAlarm is off):** Your ZoneAlarm settings are not the cause of your connection problems. Check your router and cable connections or contact your Internet source support.
   - **If yes (you *can* connect when ZoneAlarm is off):** Your ZoneAlarm settings may be the cause of your connection problem. See the troubleshooting table below for help.

If you can connect when ZoneAlarm is off and...	See...
Your computer uses a proxy server to connect to the Internet and you can't connect to the Internet	Connecting through a proxy server (on page 174)
You cannot connect to the Internet immediately after an installation	Granting a program Internet permission (to make sure your browser has access permission)
You can connect to the Internet but are disconnected after a short time	Allowing ISP Heartbeat messages (on page 174)
None of the above help	Please contact Technical Support live chat on another computer (or web-browsing phone) at http://www.zonealarm.com/chat http://www.zonealarm.com/chat

Troubleshooting Internet connection problems

Connecting through a proxy server

If you connect to the Internet through a proxy server and you are unable to connect to the Internet, make sure that the IP address of your proxy server is in your Trusted Zone.

The easiest way to add the server to the Trusted Zone is to go to **Tools | Logs | Log Viewer**, and look for the proxy server in the logs. Right-click it and choose **Add to Zone > Trusted**.

Connecting to the Internet fails after installation

If you are unable to connect to the Internet after installing ZoneAlarm security software, the first troubleshooting step is to determine whether ZoneAlarm security software is the cause. If you are unable to follow the steps below, for example, if you can't clear the **Load ZoneAlarm security software at startup** check box, contact ZoneAlarm technical support.

If you are having difficulty connecting to the Internet, first see whether ZoneAlarm is related to your Internet disconnection by trying to connect when ZoneAlarm is off:

1. Right-click the ZoneAlarm icon in the Windows taskbar notification area and choose **Shutdown**... .
2. Can you connect with ZoneAlarm off?
    - **If no (you cannot connect when ZoneAlarm is off):** Your ZoneAlarm settings are not the cause of your connection problems. Check your router and cable connections or contact your Internet source support.
    - **If yes (you *can* connect when ZoneAlarm is off):** Your ZoneAlarm settings may be the cause of your connection problem.

Allowing ISP Heartbeat messages

Internet Service Providers (ISPs) periodically send heartbeat messages to their connected dial-up customers to make sure they are still there. If the ISP cannot determine that the customer is there, it might disconnect them so that the IP address can be given to someone else.

By default, ZoneAlarm security software blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet.

To prevent this from happening, you can identify the server sending the messages and add it to your Trusted Zone or you can configure the Public Zone to allow ping messages, using one of these methods:

- Identifying the source of heartbeat messages (more secure)
- Configuring ZoneAlarm security software to allow ping messages

Identifying the source of the heartbeat messages (recommended)

This is the preferred solution because it will work whether your ISP uses NetBIOS or *ICMP (Internet Control Message Protocol)* to check your connection, and it allows you to maintain high security for the Public Zone.

To identify the server your ISP uses to check your connection:

1. When your ISP disconnects you, click **Alerts & Logs**|**Log Viewer**.
2. In the alerts list, find the alert that occurred at the time you were disconnected.
3. In the Entry Detail area, note the Source DNS detected.

   If you're not able to identify the server this way, contact your ISP to determine which servers need access permission.
4. After you have identified the server, add it to the Trusted Zone.

   See Adding to the Trusted Zone (on page 30).

Configuring ZoneAlarm security software to allow ping messages

If your ISP uses ICMP echo (or ping) messages for connectivity checks, configure ZoneAlarm security software to allow ping messages from the Public Zone.

To configure ZoneAlarm security software to allow ping messages:

1. Select **COMPUTER | Advanced Firewall**.
2. In the Public Zone area, click **Custom**.
3. Select check box labeled **Allow incoming ping (ICMP echo)**.
4. Click **OK**.
5. Set the security level for the Public Zone to Medium.

Troubleshooting Anti-virus

If you are having difficulty connecting using anti-virus software refer to the table for troubleshooting tips provided in this section.

If...	See...
An application you trust has been quarantined.	If a safe application has been quarantined
Anti-virus Monitoring feature is unavailable	Anti-virus Monitoring alert (on page 176)
You receive an alert about conflicting products	Resolving conflicts with anti-virus products (on page 176)

If...	See...
You are unable to turn on the Anti-virus feature	E-mail scanning is unavailable (on page 177)

Troubleshooting ZoneAlarm Anti-virus problems

If a safe application has been quarantined

On rare occasions, it's possible that an application you trust is quarantined because it is a spoof of the real application and therefore was detected as a virus. But, if an application that you know to be safe is quarantined, it may be a false positive virus detection. False positives occur when a pattern of code in the file matches the same pattern contained in a virus signature. This can occur due to a faulty signature or it can occur after incomplete treatment by another anti-virus scanner. False positives are most likely to occur in applications that are not widely used.

If you believe your application has been improperly quarantined, here's how to restore it and stop putting it in quarantine:

1. Select **COMPUTER | Anti-virus & Anti-Spyware| Settings |View Quarantine**.
2. Select your item under **Quarantine** and click the **Restore** button.
3. Click **Exceptions**.
4. Click **Add file...** and browse to select the trusted program that you do not want quarantined in a virus scan.
5. Click **OK** to close Add File and then to close Advanced Options.

Anti-virus Monitoring alert

The Anti-virus Monitoring alert lets you know when the anti-virus protection on your computer is not fully protecting you from viruses. You may receive this alert when your anti-virus is turned off, when your anti-virus signatures are not up-to-date, or when you are not running any anti-virus software at all.

Note that not all anti-virus products are monitored, so the absence of an alert does not necessarily mean you are protected. To ensure your protection, open your anti-virus software (if it is installed) and perform an update or renew your subscription, if it has expired.

Resolving conflicts with anti-virus products

If you also have another anti-virus product installed, you may receive a conflict alert that states you must uninstall that product before using ZoneAlarm anti-virus. The alert will list the anti-virus software products that were detected and specify whether ZoneAlarm is able to uninstall them automatically, or if they must be uninstalled manually. If the products listed cannot be uninstalled automatically, refer to the individual vendor's documentation for instructions for uninstalling the products.

E-mail scanning is unavailable

If you are attempting to enable the e-mail scanning option of ZoneAlarm anti-virus software and are unable to do so, you may have a product installed that uses Layered Service Provider (LSP) technology that is incompatible with ZoneAlarm. To remedy this situation, you will need to uninstall the conflicting product(s).

When a conflict occurs, a file called lspconflict.txt is created and placed in the C:/Windows/Internet Logs directory. This file contains the name of the product(s) that caused the conflict. You can remove the product(s) manually. Refer to the individual vendors' documentation for instructions for uninstalling the product(s).

Troubleshooting Hard Drive Encryption

For troubleshooting the *Hard Drive Encryption* feature, refer to the table below.

If...	See...
You forgot your password or username	What to do if you forget your password or username
Your system crashes and you need to recover the disk but it is encrypted	How to decrypt in case of system failure

Troubleshooting Hard Drive Encryption problems

Troubleshooting third-party software Internet access

Many of your most commonly used programs can be configured automatically for Internet access. Although, in some cases, Internet access can be configured automatically, many programs also require server access rights.

If you are using programs that ZoneAlarm security software is unable to recognize and configure automatically, you may need to configure permissions manually. Refer to the sections that follow to learn how to configure your programs for use with ZoneAlarm security software.

- Anti-virus (on page 178)
- Browsers (on page 178)
- Chat and instant messaging programs (on page 179)

- E-mail programs (on page 179)
- Internet answering machine programs (on page 179)
- File sharing programs (on page 180)
- FTP programs (on page 180)
- Games (on page 180)
- Remote control programs (on page 182)
- VNC programs (on page 182)
- Streaming media programs (on page 183)
- Voice over IP programs (on page 183)
- Web conferencing programs (on page 183)

Anti-virus

In order for your anti-virus software to receive updates it must have access permission for the Trusted Zone.

Automatic updates

In order to receive automatic updates from your anti-virus software vendor, add the domain that contains the updates (e.g., update.avsupdate.com) to your Trusted Zone. See Adding to the Trusted Zone (on page 30).

Browsers

In order for your browser to work properly, it must have access permission for the Public Zone and Trusted Zone. Before granting permission, make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

To grant your browser access permission, do any of the following:

- Grant access to the program directly. See Granting a program permission to access the Internet.
- Select **Allow** when a Program alert for the browser appears.

Internet Explorer

You may need to allow Internet access rights to the Services and Controller App (the file name is typically services.exe).

To grant Internet access permission to the Services and Controller App:

1. Select **Application Control**| **View Programs**.

2. In the Programs column, locate **Services and Controller App**.
3. In the Outbound column, select **Allow** from the shortcut menu.

Chat and instant messaging programs

Chat and instant messaging programs (for example, AOL Instant Messenger) may require server permission in order to operate properly.

To grant server permission to your chat program:

- Answer Allow to the Server Program alert caused by the program.
- Grant server permission to the program.
- See Granting a program permission to act as a server.

Important - We strongly recommend that you set your chat software to refuse file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, and Trojan horses. Refer to your chat software vendor's help files to learn how to configure your program for maximum security.

E-mail programs

In order for your e-mail program (for example, Microsoft Outlook) to send and receive mail, it must have access permission for the Zone the mail server is in. In addition, some e-mail client software may have more than one component requiring server permission. For example, Microsoft Outlook requires that both the base application (OUTLOOK.EXE) and the Messaging Subsystem Spooler (MAPISP32.exe) to have server permission.

While you can give your e-mail program access to the Public Zone, and leave the mail server there, it’s safer to place the mail server in the Trusted Zone, and limit the program's access to that Zone only. Once your e-mail client has access to the Trusted Zone, add the remote mail server (host) to the Trusted Zone.

To learn how to give a program permission to access or act as a server to the Trusted Zone, see Setting program permissions manually.

To learn how to add a host to the Trusted Zone, see Managing traffic sources (on page 29).

Internet answering machine programs

To use Internet answering machine programs (such as CallWave) with ZoneAlarm security software, do the following:

- Give the program server permission and access permission for the Public Zone.

- Add the IP address of the vendor's servers to the Trusted Zone.

  Note - To find the server IP address, contact the vendor's technical support.

- Set the security level for the Public Zone to Med.

File sharing programs

File sharing programs, such as Napster, Limewire, AudioGalaxy, or any Gnutella client software, must have server permission for the Public Zone in order to work with ZoneAlarm security software.

FTP programs

To use FTP (File Transfer Protocol) programs, you may need to make the following settings adjustments in your FTP client program and in ZoneAlarm security software:

- Enable passive or PASV mode in your FTP client

  This tells the client to use the same port for communication in both directions. If PASV is not enabled, ZoneAlarm security software may block the FTP server's attempt to contact a new port for data transfer.

- Add the FTP sites you use to the Trusted Zone
- Give Trusted Zone access permission to your FTP client program.

To learn how to add to the Trusted Zone and give access permission to a program, see Setting advanced security options (on page 26).

Games

In order to play games over the Internet while using ZoneAlarm security software, you may have to adjust the settings listed below.

Note - Note that you can configure ZoneAlarm security software to suppress most alerts while you are playing a game. For details, see Game Mode (on page 168).

Program permission

In order to function, many Internet games require access permission and/or server permission for the Public Zone.

The easiest way to grant access is to answer "Allow" to the program alert caused by the game program. However, many games run in "exclusive" full screen mode, which will prevent you from seeing the alert. Use any of the methods below to solve this problem.

- Set the game to run in a window
- This will allow you to see the alert, if the game is running at a resolution lower than that of your desktop. If the alert appears but you cannot respond to it because your mouse is locked to the game, press the Windows logo key on your keyboard.
- After granting the game program Internet access, reset the game to run full-screen.
- Use software rendering mode
- By changing your rendering mode to "Software Rendering," you can allow Windows to display the alert on top of your game screen. After allowing the game Internet access, you can change back to your preferred rendering device.
- Use Alt+Tab
- Press **Alt+Tab** to toggle back into Windows. This leaves the game running, but allows you to respond to the alert. Once you have allowed Internet access, press **Alt+Tab** again to restore your game.

Important - The last method may cause some applications to crash, especially if you are using Glide or OpenGL; however, the problem should be corrected the next time you run the game. Sometimes you can use Alt-Enter in the place of Alt-Tab.

Security level/Zone

Some Internet games, particularly those that use Java, applets, or other Web-based portal functionality, may not work properly when your Public Zone security level is set to High. High security will also prevent remote game servers from "seeing" your computer. To solve these problems, you can:

- Change your Public Zone security level to Medium, or
- Add the IP address of the game server you're connecting to the Trusted Zone. The game manufacturer's documentation should indicate the IP address or host name of the server.

To learn how to add a host or IP address to the Trusted Zone, see Adding to the Trusted Zone (on page 30).

Important - Trusting game servers means trusting the other players in the game. ZoneAlarm security software does not protect you from attacks instigated by fellow gamers in a trusted environment. Make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

Remote control programs

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu:

- Add the IP address(es) of the hosts or clients to which you connect to your Trusted Zone. See Adding to the Trusted Zone (on page 30).
- Add the subnet of the network you are accessing remotely to your Trusted Zone. See Adding to the Trusted Zone (on page 30).
- If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.

Important - If your remote control client or host is on a network not under your control (for example on a business or university LAN), perimeter firewalls or other features of the network may prevent you from connecting. If you still have problems connecting after following the instructions above, contact your network administrator for assistance.

VNC programs

In order for VNC and ZoneAlarm security software to work together, follow the steps below.

1. On both the server and viewer (client) machine, do one of the following:
   - If you know the IP address or subnet of the viewer (client) you will be using for remote access, and it will always be the same, add that IP or subnet to the Trusted Zone. See Adding to the Trusted Zone (on page 30).

If you do not know the IP address of the viewer, or if it will change, then give the program access permission and server permission for the Trusted and Public Zones. See Setting permissions for specific programs (on page 111).

When prompted by VNC Viewer on the viewer machine, enter the name or IP address of the server machine, followed by the password when prompted. You should be able to connect.

Important - If you enable VNC access by giving it server permission and access permission, be sure to set and use your VNC password in order to maintain security. We recommend adding the server and viewer IP addresses to the Trusted Zone, rather than giving the application Public Zone permission, if possible.

1. On the viewer (client) machine, run VNC Viewer to connect to the server machine. Do not run in "listen mode."

Telnet

To access a remote server via Telnet, add the IP address of that server to your Trusted Zone.

Streaming media programs

Applications that stream audio and video, such as RealPlayer, Windows Media Player, QuickTime, etc., may need server permission for the Public Zone in order to work with ZoneAlarm security software.

To learn how to give server permission to a program, see Granting a program permission to act as a server.

Voice over IP programs

To use Voice over IP (VoIP) programs with ZoneAlarm security software, you must do one or both of the following, depending on the program:

1. Give the VoIP application server permission and access permission.
2. Add the VoIP provider’s servers to the Trusted Zone. To learn the IP addresses of these servers, contact your VoIP provider's customer support.

Web conferencing programs

If you experience problems using a Web conferencing program such as Microsoft NetMeeting, try the following:

1. Add the domain or IP address that you connect to in order to hold the conference to the Trusted Zone. See Adding to the Trusted Zone (on page 30).
2. Disable the conferencing program’s "Remote Desktop Sharing" option.

Keyboard shortcuts

Global function shortcuts

Use the following keystrokes to activate functions from multiple locations in the interface. Note that some keystrokes may have other functions in specific panels. Those cases are listed under Button Shortcuts, below.

Keystroke	Function
ALT+C	Opens a Custom dialog box, where one is available.
ALT+U	Opens a second Custom dialog box, where two Custom buttons are available (for example, in the main panel of the Program ControlApplication Control panel).
ALT+A	Opens an advanced dialog box, where one is available.
ALT+DOWN ARROW	Opens the active drop-down list box. In list views, opens the left-click shortcut menu if one is available.
SHIFT+F10	In list views, opens the right-click shortcut menu if one is available.
ESC	Equivalent to clicking a Cancel button.
ENTER	Equivalent to clicking the active button.
ALT+P	Equivalent to clicking an Apply button.
Delete	Removes a selected item from a list view.
ALT+F4	Shuts down ZoneAlarm security software.

Global shortcuts

Dialog box commands

Use the keystrokes below when a dialog box is open.

Keystroke	Function
Tab	Activates the next control in the dialog box.
SHIFT+TAB	Activates the previous control in the dialog box.
CTRL+TAB	Opens the next TAB in a multiple-TAB dialog box.
CTRL+SHIFT+TAB	Opens the previous TAB in a multiple-TAB dialog box.
ALT+DOWN ARROW	Opens the active drop-down list box.
SPACEBAR	Clicks an active button. Selects/clears an active check box.
ENTER	Same as clicking the active button
ESC	Same as clicking the Cancel button.

Dialog box shortcuts

Button shortcuts

Use the keystrokes below to click available buttons in an active window.

Panel	Pane	Keystroke	Equivalent to clicking
Main	Product Info	Alt + I	Change License
Main	Product Info	Alt + B	Buy Now
Main	Product Info	Alt + N	Renew
Main	Product Info	Alt + R	Change Reg.
Main	Preferences	Alt + P	Set Password
Main	Preferences	Alt + B	Backup
Main	Preferences	Alt + R	Restore
Main	Preferences	Alt + O	Log In/Log Out

Panel	Pane	Keystroke	Equivalent to clicking
Main	Preferences	Alt + U	Check for Update
Firewall	Main	Alt + C	Public Zone Custom
Firewall	Main	Alt + U	Trusted Zone Custom
Firewall	Main	Alt + A	Advanced
Firewall	Zones	Alt +A	Add
Firewall	Zones	Alt + R	Remove
Firewall	Zones	Alt + E	Edit
Firewall	Zones	Alt + P	Apply
Firewall	Expert	Alt + A	Add
Firewall	Expert	Alt + R	Remove
Firewall	Expert	Alt + E	Edit
Firewall	Expert	Alt + P	Apply
Firewall	Expert	Alt + G	Groups
Application Control	Main	Alt + C	Program Control Custom
Application Control	Main	Alt + U	Automatic Lock Custom
Application Control	Main	Alt + A	Advanced
Application Control	Programs	Alt + A	Add
Application Control	Programs	Alt + O	Options
Application Control	Components	Alt + M	More info
Anti-virus / Anti-spyware	Main	ALT + S	Scan for Viruses/Spyware
Anti-virus / Anti-spyware	Main	ALT + U	Update Now

Panel	Pane	Keystroke	Equivalent to clicking
Anti-virus / Anti-spyware	Main	ALT + A	Advanced Options
Anti-virus / Anti-spyware	Main	ALT + V	Scan for Viruses
Anti-virus / Anti-spyware	Quarantine	ALT + D	Delete
Anti-virus / Anti-spyware	Quarantine	ALT + E	Restore
Anti-virus / Anti-spyware	Quarantine	ALT + M	More Info
E-mail Protection	Main	ALT + A	Advanced
E-mail Protection	Attachments	ALT + C	Check All
E-mail Protection	Attachments	ALT + R	Clear All
E-mail Protection	Attachments	ALT + A	Add
E-mail Protection	Attachments	ALT + P	Apply
ID Lock	myVAULT	Alt + A	Add
ID Lock	myVAULT	Alt + O	Options
ID Lock	myVAULT	Alt + N	Encrypt
ID Lock	myVAULT	Alt + E	Edit
ID Lock	myVAULT	Alt + R	Remove
ID Lock	Trusted Sites	Alt + A	Add
ID Lock	Trusted Sites	Alt + R	Remove
Alerts & Logs	Main	Alt + D	Reset to Default
Alerts & Logs	Main	Alt + C	Custom
Alerts & Logs	Main	Alt + A	Advanced

Panel	Pane	Keystroke	Equivalent to clicking
Alerts & Logs	Log Viewer	Alt + M	More Info
Alerts & Logs	Log Viewer	Alt + D	Clear List
Alerts & Logs	Log Viewer	Alt + A	Add to Zone
Alerts & Logs	Log Control	Alt + B	Browse
Alerts & Logs	Log Control	Alt + E	Delete Log

Keystrokes for activating buttons

Index

A

About alerts and managing them • 47
About myVAULT • 153
About the DataLock Settings Panel • 159
About updating from a prior version • 17
About Wireless Network Configuration • 19
Access permission • 156
Accessing technical support • 17
Action • 45
Active • 112
Adding a program to the programs list • 115
Adding a VPN gateway and other resources to the Trusted Zone • 23
Adding contacts to the Allowed List • 142
Adding custom ports • 34
Adding data to myVAULT • 153
Adding to the Blocked Zone • 32
Adding to the Trusted Sites list • 156
Adding to the Trusted Zone • 31
Advanced Program alert • 79
Allowing e-mail from distribution lists • 143
Allowing ISP Heartbeat messages • 175
Allowing or blocking e-mail from specific companies • 142
Allowing or blocking e-mail from specific senders • 142
Allowing VPN protocols • 24
Anti-virus • 179
Anti-virus Monitoring alert • 177
Application Control • 101
Archiving log entries • 168
Automatic updates • 179
Automatic VPN Configuration alert • 82
Automatic VPN detection delay • 172

B

Backing up and restoring your ZoneAlarm settings • 15
Blocked Program alert • 54
Blocking and unblocking ports • 33
Browser security • 121
Browsers • 179
Button shortcuts • 186

C

Challenging e-mail from unknown senders • 146
Changed Program alert • 70
Chat and instant messaging programs • 180
Choosing a scan mode • 126
Choosing security levels • 26
Clear Text password • 156
Collaborative Filter • 145
Configuration • 13
Configuring a new network connection • 18
Configuring for networks and resources • 18
Configuring on-access scanning • 126
Configuring OSFirewall protection • 107
Configuring your VPN connection • 21
Configuring your VPN connection automatically • 22
Configuring your VPN connection manually • 22
Configuring ZoneAlarm security software for VPN traffic • 171
Configuring ZoneAlarm security software to allow ping messages • 176
Connecting through a proxy server • 175
Connecting to network mail servers • 20
Connecting to the Internet fails after installation • 175
Controlling the number of alerts • 163
Creating a day/time group • 44
Creating a location group • 40
Creating a protocol group • 41
Creating an expert rule for a Program • 120
Creating expert firewall rules • 37
Creating expert rules for programs • 120
Creating groups • 40
Custom Application Control features • 106
Customizing behavioral scanning • 130
Customizing event logging • 164
Customizing junk email filter settings • 147
Customizing Outbound MailSafe protection • 140

Customizing program logging • 164
Customizing virus protection options • 124

D

Default port permission settings • 34
Destination • 46
Detail • 133
Dialog box commands • 185
Disabling Outbound Mail protection for a program • 118

E

Editing and removing myVAULT contents • 155
Editing and removing trusted sites • 157
Editing and re-ranking rules • 47
E-mail programs • 180
E-mail protection • 139
E-mail scanning is unavailable • 178
E-mail transmission • 150
Enabling and disabling Anti-virus Monitoring • 137
Enabling Component Control • 108
Enabling file and printer sharing • 20
Enabling Internet Connection Sharing • 21
Enabling Outbound MailSafe protection • 139
Enabling Outbound MailSafe protection by program • 140
Excluding items from virus scans • 129
Expert firewall rule enforcement rank • 37
Expert firewall rules and program permissions • 37
Expert rules and Zone rules • 36

F

File sharing programs • 181
Filtering junk e-mail (spam) • 141
Firewall alerts/Protected • 48
Firewall protection • 25
Firewall zone basics • 10
Foreign language filters • 145
Formatting log appearance • 164
FTP programs • 181

G

Game Mode • 169
Games • 181
Getting started with ZoneAlarm • 7
Global function shortcuts • 185
Granting a program permission to access the Internet • 116
Granting a program permission to act as a server • 116
Granting access permission to VPN software • 24
Granting send mail permission to a program • 117

H

High security setting • 11
High-rated Suspicious Behavior alert • 92
How expert firewall rules are enforced • 36
How to decrypt in case of system failure • 160
How to see fewer of these alerts • 51, 54, 57, 60, 63, 67, 70, 73, 76, 79, 82, 85, 88, 101
How your personal information is protected • 150

I

ID Lock alert • 98
Identifying the source of the heartbeat messages (recommended) • 176
Identity Protection Center (US only) • 157
If a safe application has been quarantined • 177
IM transmission • 151
Information • 133
Informational alerts • 48
Installing ZoneAlarm DataLock • 158
Integrating with network services • 20
Internet answering machine programs • 180
Internet Explorer • 179
Internet Lock alert • 57

K

Keeping virus definitions up-to-date • 123
Keyboard shortcuts • 185

L

Licensing, registration, and support • 16

M

MailSafe alert • 51
Making your computer visible on your local network • 172
Malicious behavior alert • 95
Managing Alerts and Logs • 160
Managing Expert Firewall Rules • 44
Managing program components • 119
Managing traffic sources • 30
Manual Action Required alert • 86
Medium security setting • 11
Medium-rated Suspicious Behavior alert • 89
Message Filters • 145
Modifying traffic sources • 31
Monitoring antivirus status alerts • 137
Monitoring Coverage • 136
Monitoring product status • 137
Monitoring virus protection • 136
Moving to a different computer • 18

N

Name • 46, 132
New Program alert • 64
Notification icons and shortcut menus • 9

O

OSFirewall alerts • 89
Outbound and Inbound • 113
Outbound MailSafe protection • 139
Overview of main features • 7

P

Path • 132
Performing a scan • 130
Program alerts • 63, 103
Program Component alert • 73
Program permission • 182
Programs • 112
Programs list • 104
Protocol • 46

R

Rank • 45
Remote alert • 60
Remote control programs • 183
Removing a VPN gateway from a blocked range or subnet • 24
Removing expert rules • 121
Renewing your product license • 17
Repairing files in an archive • 134
Repeat Program alert • 67
Reporting junk email • 143
Reporting phishing email • 144
Resolving a slow start up • 173
Resolving conflicts with anti-virus products • 177
Responding to alerts • 12
Restoring e-mail incorrectly identified as junk • 149
Rootkit scanning • 131

S

Safe programs • 103
Scanning your Inbox • 143
Scheduling regular anti-virus scans • 123
Security level/Zone • 182
Security Risk • 132
Send Mail • 114
Server • 114
Server Program alert • 76
Setting Advanced Application Control options • 117
Setting advanced security options • 27
Setting authentication options • 118
Setting basic alert and log options • 162
Setting event and program log options • 163
Setting event and program logging options • 162
Setting general product preferences • 15
Setting general program control options • 104
Setting general security options • 27
Setting network security options • 28
Setting Outbound MailSafe protection options • 140
Setting passlock permission for a program • 119
Setting permissions for specific programs • 112
Setting product preferences • 14
Setting product update options • 16
Setting program options for a specific program • 117

Setting program permissions automatically • 102
Setting program permissions manually • 103
Setting the alert event level • 162
Setting the ID Lock protection level • 152
Setting the program control level • 104
Setting the security level for a Zone • 26
Setting the SmartDefense Advisor level • 109
Setting wireless network security options • 29
Setting your password • 14
Sharing files and printers across a local network • 173
Showing or hiding firewall and program alerts • 161, 163
Site • 156
Site Entry Details • 156
SmartDefense Advisor • 113
Source • 46
Specifying junk e-mail message options • 145
Specifying scan options • 127
Specifying scan targets • 124
Specifying the archive location • 168
Specifying your outbound e-mail server • 147
Spyware and virus Protection • 122
Status • 132
Stopping or uninstalling ZoneAlarm DataLock • 159
Streaming media programs • 184
Supported VPN protocols • 21

T

Telnet • 184
Text log fields • 167
Time • 46
Track • 45
Treating virus files manually • 133
Treatment • 132
Troubleshooting • 171
Troubleshooting an Internet disconnection • 174
Troubleshooting Anti-virus • 176
Troubleshooting Hard Drive Encryption • 178
Troubleshooting networking • 172
Troubleshooting third-party software Internet access • 178
Troubleshooting VPN • 171
Troubleshooting VPN problems • 171
Troubleshooting ZoneAlarm DataLock • 159
Trust Level • 113
Turning Game Mode On and Off • 170
Turning on virus and spyware protection • 123
Type • 132, 156

U

Understanding alerts and logs • 161
Understanding and reducing alerts • 47
Understanding Application Control • 101
Understanding Auto-Learn • 105
Understanding e-mail protection • 139
Understanding expert firewall rules • 36
Understanding Firewall protection • 25
Understanding Game Mode • 169
Understanding services control • 108
Understanding the ID Lock feature • 150
Understanding virus scan results • 131
Uninstalling • 18
Updating your ZoneAlarm registration information • 17
Using browser security • 121
Using SmartDefense Advisor and Hacker ID • 168
Using the Network Configuration Wizard • 19
Using the programs list • 112
Using the Trusted Sites list • 155
Using ZoneAlarm DataLock • 158

V

Viewing items in quarantine • 138
Viewing junk email filter reports • 149
Viewing log entries • 165
Viewing logged Firewall events • 32
Viewing logged OSFirewall events • 111
Viewing logged program events • 110
Viewing logged virus events • 134
Viewing Status Messages in the Anti-virus Monitoring panel • 137
Viewing the Expert Rules list • 44
Viewing the text log • 166

Viewing the traffic source list • 30
Viewing the Trusted Sites list • 156
Viewing virus and spyware protection status • 135
VNC programs • 183
Voice over IP programs • 184
VPN auto-configuration and expert rules • 172

W

Web conferencing programs • 184
Web transmission • 151
Welcome • 7
What Hard Drive Encryption does for you • 158
What to do if you forget your password or username • 159
What you should do • 48, 51, 54, 58, 61, 64, 67, 70, 74, 77, 80, 83, 86, 89, 92, 95, 98
When your license expires • 16
Why these alerts occur • 48, 51, 54, 57, 60, 64, 67, 70, 73, 76, 80, 83, 86, 92, 95, 98

Z

ZoneAlarm security software basics • 7
ZoneAlarm User Forum • 7
Zones manage firewall security • 11
Zones provide Application Control as outbound protection • 12